DYADIC CORRELATION PROPERTIES OF NON-REPETITIVE QUADRATIC BOOLEAN FUNCTIONS

A Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY

By

HARPREET SINGH SAWHNEY

to the

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
JULY, 1981

. .to my
parents. .

CERTIFICATE

This is to certify that the work embodied in this thesis entitled: "DYADIC CORRELATION PROPERTIES OF NON-REPETITIVE QUADRATIC BOOLEAN FUNCTIONS" carried out by Sri Harpreet Singh Sawhney, under my supervision has not been submitted elsewhere for a degree.

M U Siddiqi
(M.U. Siddiqi) 29.7.81
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology, Kanpur

July 1981.

ACKNOWLEDGEMENT

My work has borne fruit under the able and friendly guidance of Dr. M.U. Siddiqi. I express a sense of gratitude and respect for him on this occassion. Words cannot convey the depths of my emotions towards my friends and teachers, who have made my stay at IIT, Kanpur a memorable experience. I am heavily indebted to them for my cultural and academic development. Their criticism will guide me throughout my life.

This work has been completed under the soothing support of my parents and brother. Although far away, they have always been a source of inspiration and happiness to me. I take this opportunity to convey my deeply felt regards for them.

I am extremely grateful to Mr. R.D. Singh for his excellent typing work and his endurance during some trying moments. Finally, thanks to Mr. Panditji for his help in the cyclostyling work.

HARPREET SINGH

CONTENTS

ABSTRACT

Dyadic correlation properties of a class of second degree binary Boolean functions, called NON-REPETITIVE QUADRATIC FORMS (NRQFs), are analysed using Walsh-Hadamard transform techniques. It is shown that these 2^n-point functions of n variables possess ideal dyadic auto-correlation and asymptotically ideal cross-correlation properties. Walsh-Hadamard spectral coefficients of NRQFs are found to be of uniform magnitude. It is proved that all 2^n-point functions with uniform magnitude spectral property possess ideal dyadic auto-correlation and vice-versa. Such functions are shown to be optimal as perturbation signals for identification of linear dyadic-shift invariant systems. The class of these functions, known as bent functions, are presented briefly with their properties. The NRQFs constitute a sub-class of binary bent functions. Some interesting results on dyadic correlation properties of two-dimensional arrays, synthesised using NRQFs and Walsh functions, are derived. For comparison with linear-feedback shift-register (LFSR) sequences which are known to possess good periodic and aperiodic correlation properties, periodic and aperiodic correlation parameters of some NRQFs are computed. Minimal LFSR circuit realizations of NRQFs are studied and their complexity compared with maximal-length LFSR sequence generators. Finally, a method is suggested for design of binary sequences with desired dyadic correlation properties.

CHAPTER I

INTRODUCTION

Considerable research has gone into the analysis and synthesis of sequences with good correlation properties [Boehmer, 1967; MacWilliams and Sloane, 1976; Shedd and Sarwate, 1979; Sarwate and Pursley, 1980]. The resulting achievements have been both a mathematician's delight and an engineer's boon. Binary and poly-phase sequences, both have attracted researchers. However, the focus of attention have been binary sequences as they are easily generated using the available hardware. Two level sequences with good cyclic and linear correlation properties find many applications in their respective domains. From the more abstract systems' viewpoint, correlation, defined in a given way, is closely related to systems characterised by input-output convolution relations defined in a similar way. Further, correlation analysis can be performed in the transform domain using the system-specific transform. Consequently, both the sample domain and the transform domain properties of sequences are of use in their correlation studies.

Binary sequences synthesised using linear-feedback shift-register (LFSR) configurations are mathematically elegant, easily generated and rich in their potential for use in various applications [Golomb, 1964; Golomb, 1967]. A sub-class of these, called maximal-length sequences (m-sequences) or pseudo-random binary sequences (PRBSs), possess asymptotically ideal linear (aperiodic) and cyclic (periodic) correlation properties. They have found extensive use, traditionally, in Radar Ranging [Golomb, 1964], Cryptography [Geffe, 1973; Feistal et al., 1975] and Scrambling [Henriksson, 1972], and, more recently, as wide-band signature sequences in Spread-Spectrum Code-Division Multiple-Access (SS-CDMA) communication systems [Pursley and Sarwate, 1977; Pursley and Roefs, 1979]. Actually, large sets of sequences, known as Gold [Gold, 1968] and Kasami [Sarwate and Pursley, 1980] sequences derived from a combination of m-sequences are used for SS-CDMA systems. m-sequences, owing to their good auto-correlation property, constitute a near-ideal set of signals for identification of linear cyclic-shift invariant (LCSIV) systems. Cyclic convolution and discrete Fourier transform (DFT) relate the input and output of these systems in the sample and transform domains, respectively. DFT row vectors are their eigensignals. Hence, cyclic correlation analysis of LFSR and other sequences can be performed using DFT techniques. Non-binary poly-phase sequences possessing ideal cyclic correlation are also known. These are the Frank-Zadoff-Chu (FZC) sequences [Frank and Zadoff, 1962; Chu, 1972].

Some of the well known sequences having near-optimal aperiodic correlation properties are Barker (binary) and Huffman (non-binary) sequences [Huffman, 1962]. Unfortunately, binary Barker sequences are known to exist only upto length 13. Generalized Barker sequences [Golomb and Scholtz, 1965] and Huffman sequences are of not much use practically. Hence, other sub-optimal binary sequences - viz. pulse compression codes [Boehmer, 1967], even-shift orthogonal sequences [Taki and Miyakawa, 1969] etc. - have also been studied.

1.1 SCOPE OF THE PRESENT WORK

The present work is devoted to correlation analysis of a class of binary sequences with good dyadic correlation properties. Dyadic correlation analysis uses Walsh-Hadamard transform (WHT) techniques because Walsh functions are eigen-signals for linear dyadic-shift invariant (LDSIV) systems whose output is dyadic convolution/correlation between the input and the system sample vector. Accordingly, WHT techniques are applied to a class of n variable 2^n-point binary Boolean functions called NON-REPETITIVE QUADRATIC FORMS (NRQFs) [Karpovsky, 1976], for study of their dyadic correlation properties. WHT coefficients of NRQFs are computed by correlating them (NRQFs) with linear Boolean functions (LBFs), as each row of an $N \times N$ ($N = 2^n$) Walsh-Hadamard matrix is one of 2^n LBFs of n variables. The WHT coefficients turn out to be of uniform magnitude, $2^{n/2}$. Uniform magnitude sequency-spectrum results in the 2^n-point $\{+1, -1\}$-valued NRQFs having ideal dyadic auto-correlation. Thus, they constitute an ideal set of perturbation signals for identification of LDSIV systems. NRQFs constitute a sub-class of another known set of functions, called BENT FUNCTIONS, which have the uniform spectral property. These have also been presented briefly.

Further, cross-correlation properties of NRQFs are derived. They are shown to be asymptotically ideal. This has been achieved using the permutation cycle structure relationships between NRQFs. An important result relating cross-correlation function of two NRQFs to the cross-correlation functions of each of these with a third NRQF, is derived.

In order to compare the correlation performance of NRQFs vis-a-vis m-sequences, periodic and aperiodic correlation parameters of some typical NRQFs are computed. However, they turn out to be considerably worse. Another parameter for comparison is the complexity of minimal LFSR circuits as NRQF generators vis-a-vis m-sequence LFSR synthesizers. Number of stages of minimal LFSR circuits needed to generate NRQFs of 2, 4, 6 and 8 variables are computed using Massey's shift-register synthesis algorithm [Massey, 1969].

Taking a cue from the one-to-one relationship between existence of certain integer difference sets and sequences with good cyclic auto-correlations (m-sequences etc.) [Meetham, 1969], a method is suggested for design of sequences with desired dyadic auto-correlation properties using what have been defined as dyadic difference sets.

Finally, dyadic correlation properties of NRQFs and Walsh functions are utilized for synthesis of two-dimensional $\{+1, -1\}$-valued arrays with good correlation properties. Two methods of synthesis are presented and the resulting correlations derived. A judicious choice of NRQFs and Walsh functions as the component arrays leads to some interesting results.

1.2 ORGANISATION OF THE THESIS

In Chapter 2, we present an integrated brief review on sequences with good periodic and aperiodic correlation properties. Beginning with the definition of periodic correlation, we relate it to the DFTs of the component arrays and derive certain conditions to be satisfied by their DFTs for the arrays to possess ideal auto- and cross-correlations. FZC and Nth roots of unity - sequences are presented next as specific instances of sequences with good periodic correlation properties. Then, we go on to a brief exposition of m-sequences - their generation and some important properties. Their asymptotically ideal auto-correlation is related, next, to their DFTs. An overview of important properties of LCSIV systems and a scheme for their identification are given. The chapter ends with a brief review of sequences with good aperiodic correlation properties.

In Chapter 3, we present an overview of dyadic correlation and LDSIV systems. Dyadic correlation/convolution and their relation to LDSIV systems is given which is followed by some of their elementary properties in terms of the Walsh-Hadamard transform. A scheme for the identification of LDSIV systems is presented next. A typical dyadic correlator configuration used in the scheme is also presented. Finally, a note on WHT-based classification of Boolean functions is added as an aid to dyadic correlation analysis in Chapter 4.

Chapter 4 is a detailed presentation of non-repetitive quadratic forms (NRQFs). Beginning with their definition, elementary properties and method of generation using counters, minimal LFSR circuit realisations of some typical NRQFs are tabulated next. Then, WHT coefficients of NRQFs are derived. These are used to analyse their auto- and cross-correlation properties in detail. Finally, aperiodic and periodic correlation parameters of a few NRQFs of 4, 6 and 8 variables are presented.

Bent functions, a generalisation of NRQFs, are reviewed in Chapter 5. Important properties of these functions are presented. Scope for enumeration of bent functions of a given number of variables is also analysed. Quadratic bent functions are given as a special class of bent functions which can be completely and easily enumerated. The chapter ends with proving the ideal auto-correlation property of bent functions.

Chapter 6, the concluding chapter, summarises the achievements of this work. Certain related directions for further endeavours are suggested. Further groundwork is needed for these to lead to certain conclusive results.

CHAPTER 2

SEQUENCES WITH GOOD PERIODIC AND APERIODIC CORRELATION PROPERTIES

This chapter is a review of linear cyclic-shift invariant systems, DFT and sequences with good periodic and aperiodic correlation properties. Beginning with a definition of cyclic correlation in Section 2.1 and introduction of the DFT approach to its analysis, conditions on DFTs of sequences with ideal correlations are derived in Section 2.1.1. Section 2.1.2 gives FZC and Nth roots of unity - sequences as instances of sequences possessing the required DFTs for ideal auto-correlation and ideal cross-correlation, respectively. Section 2.2 is a brief exposition of m-sequences - their generation and a few important properties. Their asymptotically ideal auto-correlation and the required DFTs are also presented. This DFT approach to m-sequences is rare in literature. LCSIV systems, their elementary properties and a scheme for their identification using m-sequences constitute Section 2.3. Finally, Section 2.4 with a brief overview of sequences with good aperiodic correlation properties marks the end of this chapter.

2.1 CYLIC/PERIODIC CORRELATION

We begin with the preliminaries of defining cyclic or periodic correlations. In general, given two N-length complex-valued sequences:

$$\underline{u} = (u_o u_1 \;.....\; u_{N-1})$$

$$\underline{v} = (v_o v_1 \;.....\; v_{N-1}),$$

the cyclic shift by s of $\underline{u}$ is

$$T^s\underline{u} = (u_{N-s}, u_{N-s+1}, ..., u_{N-1}, u_o, u_1, ... u_{N-1-s})$$

i.e. $(T^s\underline{u})_i = u_{i-s}$, $(i-s)$ mod N.

The periodic auto-correlation for any cyclic shift is defined as:

$$p_u(s) = \langle \underline{u}, T^s\underline{u}^* \rangle = \sum_{i=0}^{N-1} u_i \, u^*_{i-s} \;, \quad (i-s) \bmod N,$$

$$s = 0, 1, \ldots (N-1), \qquad (2.1)$$

where $\langle \; , \; \rangle$ denotes the inner product of the component sequences and '*' is the complex-conjugation.

Similarly, cyclic cross-correlation between $\underline{u}$ and $\underline{v}$ is:

$$p_{uv}(s) = \langle \underline{u}, T^s\underline{v}^* \rangle = \sum_{i=0}^{N-1} u_i v^*_{i-s} \;, \quad (i-s) \bmod N,$$

$$s = 0, 1, \ldots (N-1) \qquad (2.2)$$

As is evident from the definition,

$$p_u(s+N) = p_u(s) \text{ and } p_{uv}(s+N) = p_{uv}(s) \qquad (2.3)$$

Of prime interest here are ideal and asymptotically ideal (near-ideal) correlations and the sequences possessing them. A sequence $\underline{u}$ is said to possess ideal periodic auto-correlation if:

$$p_u(s) = \begin{cases} N \ , & s = 0 \\ 0 \ , & s = 1, 2, \ldots, (N-1), \end{cases} \qquad (2.4)$$

i.e. if the sidelobes are identically equal to zero.

Ideal cross-correlation between $\underline{u}$ and $\underline{v}$ implies that:

$$p_{uv}(s) = 0 \ , \text{ for all } s = 0, 1, \ldots, (N-1). \qquad (2.5)$$

The requirements for these ideal correlations can also be translated into certain conditions to be satisfied by the DFTs of the component sequences. The DFT of an N-length array

$$\underline{\underline{x}} = (x_o x_1 \ldots\ldots x_{N-1})^T$$

is defined as:

$$X(s) = \frac{1}{N} \sum_{i=0}^{N-1} x_i \exp(-j \frac{2\pi si}{N}),$$

$$s = 0, 1, \ldots, (N-1) \qquad (2.6)$$

In the matrix form, this is:

$$\underline{\underline{X}} = \frac{1}{N} \underline{\underline{F}} \underline{\underline{x}} , \qquad (2.7)$$

where

$$\underline{\underline{F}} = \begin{bmatrix} 1 & & & \cdots\cdots & 1 \\ 1 & a & a^2 & \cdots\cdots & a^{N-1} \\ 1 & a^2 & a^4 & \cdots\cdots & a^{N-2} \\ \cdot & & & & \\ \cdot & & & & \\ 1 & a^{N-1} & a^{N-2} & \cdots\cdots & a \end{bmatrix}, \quad a = \exp(-j \frac{2\pi}{N})$$

is the N x N DFT matrix with 'a' as the Nth root of unity.

$$\underline{x} = \underline{\underline{F}}^* \, \underline{X} \tag{2.8}$$

is the inverse DFT of $\underline{X}$.

DFT of the correlation function $\underline{p}_{uv}$ is:

$$P_{uv}(k) = \frac{1}{N} \sum_{s=0}^{N-1} p_{uv}(s) \exp(-j \frac{2\pi ks}{N})$$

$$= \frac{1}{N} \sum_{s=0}^{N-1} (\sum_{i=0}^{N-1} u_i v^*_{i-s}) \exp(-j \frac{2\pi ks}{N})$$

Substitute i-s = t, then,

$$P_{uv}(k) = \frac{1}{N} \sum_{i=0}^{N-1} u_i \sum_{t=0}^{N-1} v^*_t \exp(-j \frac{2\pi k(i-t)}{N})$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} u_i \exp(-j \frac{2\pi ik}{N}) \sum_{t=0}^{N-1} v^*_t \exp(+j \frac{2\pi kt}{N})$$

$$= N \cdot U_k \cdot V^*_k \tag{2.9}$$

where $\underline{U}$ and $\underline{V}$ are the DFTs of $\underline{u}$ and $\underline{v}$, respectively.

Hence, $\underline{P}_{uv} = N\ (\underline{U} \cdot \underline{V}^*)$ (2.10)

where $\underline{U} = \frac{1}{N}\ \underline{\underline{F}}\ \underline{u}$ and $\underline{V}^* = \frac{1}{N}\ \underline{\underline{F}}^*\ \underline{v}^*$.

Thus, $\underline{p}_{uv} = N\ \underline{\underline{F}}^*\ (\underline{U} \cdot \underline{V}^*)$ (2.11)

This can be stated as a Lemma.

Lemma 2.1:

The cyclic correlation between two complex valued N-length sequences $\underline{u}$ and $\underline{v}$ is N times the inverse DFT of termwise product of $\underline{U}$ and $\underline{V}^*$.

Corollary 2.1:

If $\underline{u}$ and $\underline{v}$ are real-valued, then,

$\underline{P}_{uv} = N(\underline{U}.\underline{V}^*)$ and $(\underline{V}^* = \frac{1}{N}\ \underline{\underline{F}}^*\ \underline{v})$ (2.12)

$\underline{p}_{uv} = N\ \underline{\underline{F}}^*\ (\underline{U}.\underline{V}^*)$ (2.13)

Corollary 2.2:

If $\underline{u} = \underline{v}$, $\underline{p}_{uv} = \underline{p}_u$ is the auto-correlation function and thus,

$\underline{P}_u = N\ (\ \underline{U}.\underline{U}^*) \ = N\ |\underline{U}|^2$ (2.14)

2.1.1 Conditions on DFTs of Sequences for Ideal Correlations

Ideal auto-correlation, from (2.4) is:

$$\underline{p}_u = (\ N\ \ 0\ \ldots\ldots\ 0\ )^T$$

For $\underline{u}$ to possess it, it is necessary that:

$$\underline{P}_u = N \left| \underline{U} \right|^2 = \frac{1}{N} \underline{\underline{F}}\, \underline{p}_u$$

$$\text{or } \left|\underline{U}\right|^2 = \frac{1}{N^2} \underline{\underline{F}}\, \underline{p}_u$$

$$= \frac{1}{N^2} \underline{\underline{F}} \cdot (N \quad 0 \; \ldots \; 0)^T$$

$$= \frac{1}{N^2} \cdot N \; (1 \; 1 \; \ldots\ldots \; 1)^T$$

$$\text{so, } \left|\underline{U}\right| = \left(\frac{1}{N}\right)^{\frac{1}{2}} (\; 1 \; 1 \; \ldots\ldots \; 1)^T$$

Lemma 2.2:

A necessary and sufficient condition for a complex-valued N-length sequence $\underline{u}$ to have ideal cyclic auto-correlation is:

$$U_i = \left(\frac{1}{N} \right)^{\frac{1}{2}} \exp(ja_i), \quad a_i \text{ arbitrary,}$$

i.e. each spectral component U_i of $\underline{u}$ should have uniform magnitude $\left(\frac{1}{N} \right)^{\frac{1}{2}}$.

Similarly, ideal cross-correlation, from (2.5), is:

$$\underline{p}_{uv} = (0 \; 0 \; \ldots\ldots \; 0)^T$$

$$\text{so} \quad \underline{P}_{uv} = N(\underline{U}.\underline{V}^*)$$

$$= \frac{1}{N} \underline{\underline{F}}\, \underline{p}_{uv}$$

$$= (0 \; 0 \; \ldots\ldots \; 0)^T$$

$$\text{or} \quad \underline{U}.\underline{V}^* = (0 \; 0 \; \ldots\ldots \; 0)^T$$

Lemma 2.3:

Two N-length complex-valued sequences $\underline{u}$ and $\underline{v}$ possess ideal cyclic cross-correlation iff for each i, either one or both of U_i and V_i are zero.

These results indicate the transform approach to correlation analysis. Conditions for ideal correlations have been specified.

Thus, ideal cyclic correlation sequences should possess the appropriate DFTs. Ideally, sequences with both ideal auto- and cross-correlations are desired. No known sequences possess both these assets. A class of poly-phase sequences called the Frank-Zadoff-Chu (FZC) sequences and Nth roots of unity sequences are known to possess ideal auto- and cross-correlations, respectively. These are discussed in the next section.

2.1.2 FZC and Nth Roots of Unity - Sequences

FZC sequences for length N are defined as follows [Chu, 1972]:

Define M

(i) If N is even and gcd (M,N) = 1,

$$\text{then } u_k = \exp\left(j \frac{\pi M k^2}{N}\right)$$

(ii) If N is odd and gcd (M,N) = 1,

$$\text{then } u_k = \exp\left(j \frac{\pi M k(k+1)}{N}\right).$$

Example 2.1: For instance, consider the 4-length sequence (M=1):

$u_o = 1,\ u_1 = \exp(j\ 45°),\ u_2 = -1,\ u_3 = \exp(j\ 45°).$

The DFT, $\underline{U}$, of this sequence is:

$\underline{U} = (\tfrac{1}{2} \exp\ (j\ 45°) \quad \tfrac{1}{2} \quad \tfrac{1}{2} \exp(j\ 135°) \quad \tfrac{1}{2})^T$

Also $\underline{p}_u = (\ 4 \quad 0 \quad 0 \quad 0\ )^T$

In general, it can be shown [Sarwate, 1979] for the FZC sequences that:

$\underline{p}_u = (N \quad 0 \quad 0\ .\ .\ .\ 0)^T$ and

$U_i = (\frac{1}{N})^{\frac{1}{2}} \exp(j a_i)$ as required by Lemma 2.2.

Similarly, another class of poly-phase N-length sequences formed using the Nth roots of unity can be seen to have ideal cross-correlation. There are a set of N such sequences for every N. Each N-length sequence is a row of the N x N DFT matrix. So, the tth element of the ith sequence,

$${}^{i}x_t = \exp(-j\ \frac{2\pi it}{N}).$$

Consider two sequences $\underline{u}$ and $\underline{v}$:

$\underline{u} = {}^{i}\underline{x}$, the ith sequence and

$\underline{v} = {}^{m}\underline{x}$, the mth sequence.

So, $u_k = \exp(-j\ \frac{2\pi ik}{N})$, $\quad v_k = \exp(-j\ \frac{2\pi mk}{N})$

$$\underline{U} = \frac{1}{N}\ \underline{\underline{F}}\ \_ = \begin{array}{cccccccc} & 0 & & i-1 & i & i+1 & & N-1 \\ (& 0 & \cdots\cdot & 0 & 1 & 0 & \cdots & 0\ )^T \end{array}$$

$$\underline{V}^* = \frac{1}{N}\ \underline{\underline{F}}^*\ \underline{v}^* = \begin{array}{cccccccc} & 0 & & m-1 & m & m+1 & & N-1 \\ (& 0 & \cdots\cdot & 0 & 1 & 0 & \cdots & 0\ )^T \end{array}$$

Thus, $(\underline{U} \cdot \underline{V}^*) = \quad (\ 0 \cdots\cdots 0 \quad 0 \quad 0 \cdots 0\ )^T$

This satisfies the condition of Lemma 2.3. Hence, these sequences are absolutely uncorrelated.

Unfortunately, these poly-phase sequences are of little applicational value as they are hard to generate. So, easily generated binary sequences with sub-optimal correlation properties are to be accepted. LFSR sequences are the most widely used such sequences. In fact , their mathematical and operational elegance leaves little else to be desired as far as cyclic correlation is concerned.

2.2 MAXIMAL-LENGTH LFSR SEQUENCES

These sequences, also called m-sequences or pseudo-random binary sequences (PRBSs), are $\{0,1\}$ or $\{+1, -1\}$ sequences generated using linear-feedback shift-register circuits. They are known to possess asymptotically ideal (near-ideal) correlation. Asymptotically-ideal auto-correlation is defined as follows:

Let $^{a}p_{max} = \{\max |p_u(s)| \; : \; 1 \leqslant s \leqslant N-1\}$,

then $\underline{u}$ has asymptotically ideal auto-correlation if:

$$\lim_{N \to \infty} \frac{^{a}p_{max}}{p_u(0)} \longrightarrow 0 \tag{2.15}$$

Before going on to their asymptotically-ideal correlation, we give some preliminaries about m-sequences.

2.2.1 Generation of m-Sequences

The general configuration of an r-stage 2^r-1 - length sequence generator LFSR circuit is as shown in Fig. 2.1.

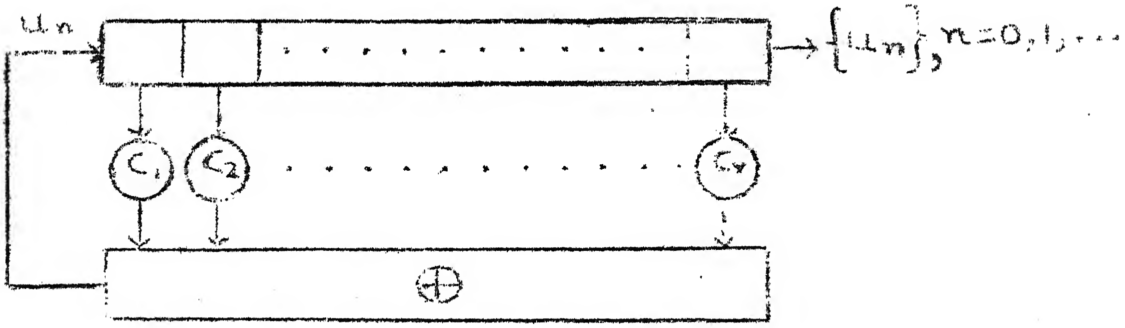


FIG. 2.1

This circuit generates the sequence $\{u_n\}$, n = 0, 1, 2,... with periodicity (2^r-1). Output u_n for an r-stage LFSR is given by the following recurrence relation as is evident from the configuration ($\sum$ is the exclusive OR summation):

$$u_n \oplus \sum_{i=1}^{r} c_i \, u_{n-i} = 0 \ , \ n \geqslant r, \ c_i \in \{0, \ 1\} \qquad (2.16)$$

Define operator D as: $Du_i = u_{i+1}$.

Then (2.16) becomes:

$$(D^r \oplus \sum_{i=1}^{r} c_i \, D^{r-i}) u_n = 0, \ n \geqslant 0 \qquad (2.17)$$

The solution of this [Key, 1976] is obtained using the extended field $GF(2^r)$ and the initial loading $(u_o u_1 \ldots . u_{r-1})$.

From (2.17), the characteristic equation of the generator is:

$$x^r \oplus \sum_{i=1}^{r} c_i \; x^{r-i} = 0 \qquad (2.18)$$

This is also the connection polynomial which specifies the configuration of the LFSR circuit. Alongwith the initial loading, it specifies the generated sequence completely. Initial state has to be a non-zero state to obtain a non-trivial solution. LFSR being a finite-state m/c, the sequence of its states has to be periodic. The maximum period of an r-stage LFSR can be 2^r-1 as the all-zero state is excluded. Hence, the name maximal-length sequences for such outputs. This shows that not all connecting polynomials generate m-sequences. In fact, a necessary and sufficient condition for m-sequence generation is that the connecting polynomial should be a primitive irreducible polynomial of GF(2^r). [Golomb, 1967]. To illustrate this, we consider two examples - one using a primitive polynomial and the other a non-primitive irreducible one.

<u>Example 2.2</u>: Consider the non-primitive irreducible polynomial:

$$x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1 \;=\; 0$$

Initial loading is (1 0 0 0).

The LFSR configuration is shown in Fig. 2.2(a) and the sequence generated is:

$$\begin{array}{llllllllll} u_0 & u_1 \ldots \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \ldots \end{array}$$

Period of the sequence is 5 and not $2^r-1 = 15$.

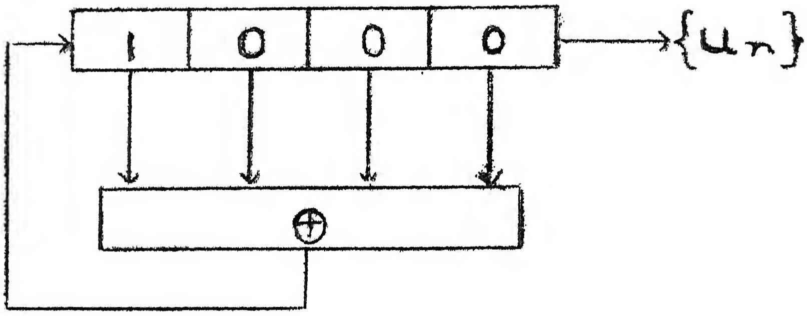


FIG 2·2(a)

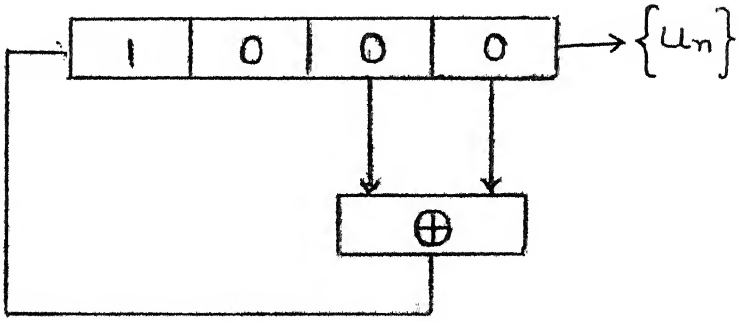


FIG 2·2(b)

Example 2.3:

The configuration of Fig. 2.2(b) is for the primitive polynomial of $GF(2^4)$:

$$x^4 \oplus x \oplus 1 = 0.$$

Initial loading is (1 0 0 0).

The generated sequence is

$u_o \; u_1 \ldots \qquad\qquad\qquad\qquad\qquad\qquad\qquad u_{14}$

0 0 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 0 1...

The period obviously is 15.

This brings us to the problem of finding the number of distinct (cyclic shifts of a sequence belong to the same equivalence class) m-sequences of length 2^r-1. This is a well known result.

Lemma 2.4 {Golomb, 1967}:

The number of distinct m-sequences of period 2^r-1 is:

$$\frac{\phi(2^r-1)}{r},$$

where $\phi(n)$ is the Euler-totient function defined as:

$$\phi(n) = \begin{cases} 1 & \text{if } n=1 \\ \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1) & \text{if } n > 1 \end{cases}$$

and by the unique factorisation theorem, every integer $n > 1$ is a product of powers of distinct primes,

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

$\phi(2^r-1)$ is the number of positive integers less than 2^r-1 and prime to it.

$\phi(2^r-1) = 2^r-2$ if 2^r-1 is a prime.

(called Mersenne prime).

Hence, for prime periods 2^r-1, the number of distinct m-sequences is:

$$\frac{2^r-2}{r} .$$

With these preliminaries of m-sequence generation, we go on to enumerate some of their important properties.

2.2.2 Properties of m-Sequences

Some of their important properties exhibiting their mathematical elegance and potential for use are:

PROPERTY 1: SHIFT PROPERTY

Cycle shift $T^s\underline{u}$ of sequence $\underline{u}$ is another m-sequence.

PROPERTY 2: SHIFT AND ADD PROPERTY

Mod 2 sum $\underline{u} \oplus T^s\underline{u}$ of a sequence and its cyclic shift is another "phase" of $\underline{u}$.

PROPERTY 3: WINDOW PROPERTY

An r-length window moved through a (2^r-1) - length m-sequence 'shows' every non-zero r-tuple exactly once.

Alternatively, each non-zero state occurs exactly once in a period of the sequence:

$$\text{e.g. } \underline{u} = 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1 \ldots$$

of example 2.3 exhibits the following sequence of states:

$$\begin{array}{l l l}
\downarrow\ 0\,0\,0\,1 & \downarrow\ 0\,1\,1\,0 & \downarrow\ 0\,1\,1\,1 \\
0\,0\,1\,0 & 1\,1\,0\,1 & 1\,1\,1\,1 \\
0\,1\,0\,0 & 1\,0\,1\,0 & 1\,1\,1\,0 \\
1\,0\,0\,1 & 0\,1\,0\,1 & 1\,1\,0\,0 \\
0\,0\,1\,1 & 1\,0\,1\,1 & 1\,0\,0\,0
\end{array}$$

PROPERTY 4: AUTO-CORRELATION PROPERTY

Consider the $\{+1, -1\}$ m-sequence $\underline{u}^c$ formed out of the $\{0, 1\}$ $\underline{u}$ using: $u_i^c = 1 - 2\,u_i$.

Then, the auto-correlation of $\underline{u}^c$ is:

$$p_{u^c}(s) = \begin{cases} N, & s = 0 \\ -1, & s = 1, 2, \ldots, (N-1). \end{cases}$$

$$\text{So, } {}^a p_{max} = 1 \text{ and } \lim_{N \to \infty} \frac{{}^a p_{max}}{p_u(0)} = \lim_{N \to \infty} \frac{1}{N} \longrightarrow 0$$

Hence, from (2.15), these sequences have near-ideal auto-correlation. This can also be seen in terms of their DFT.

For the given $p_u(s)$,

$$P_u(k) = \frac{1}{N} \sum_{i=0}^{N-1} p_u(i) \exp(-j \frac{2\pi ik}{N})$$

$$\text{(a) } P_u(k=0) = \frac{1}{N} \sum_{i=0}^{N-1} p_u(i) = \frac{1}{N} (N-(N-1)) = \frac{1}{N}.$$

(b) $$P_u(k\neq 0) = \frac{1}{N}\left(N - \sum_{i=1}^{N-1} \exp\left(-j\,\frac{2\pi ik}{N}\right)\right)$$

$$\sum_{i=1}^{N-1} \exp\left(-j\,\frac{2\pi ik}{N}\right) = -1 \text{ for } k\neq 0.$$

So, $P_u(k\neq 0) = \frac{1}{N}(N-(-1)) = \frac{1}{N}(N+1)$

Now, $P_u(k) = N|U_k|^2$

$$\text{Thus,}\quad |U_k|^2 = \begin{cases} \dfrac{1}{N^2} & ,\ k=0 \bmod N \\[2ex] \dfrac{1}{N^2}(N+1), & k\neq 0 \bmod N \end{cases} \tag{2.19}$$

Also, all sequences having (2.19) as the DFT possess the near-ideal correlation. This leads to the Lemma:

Lemma 2.5:

The periodic auto-correlation of a sequence $\underline{u}$ is of the m-sequence kind iff:

$$U_k = \begin{cases} \frac{1}{N}\exp(ja_k) & ,\ k=0 \bmod N \\[2ex] \frac{1}{N}(N+1)^{\frac{1}{2}}\exp(ja_k), & k\neq 0 \bmod N \end{cases} \qquad (a_k \text{ arbitrary})$$

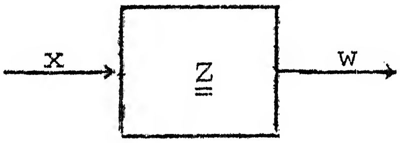
Example 2.4: Let $\underline{u} = (-1\ 1\ 1\ -1\ 1\ -1\ -1)$, $N=7$,

$$\underline{U} = \left(\frac{1}{7}e^{j180°}, \frac{2\sqrt{2}}{7}e^{j249°}, \frac{2\sqrt{2}}{7}e^{j249°}, \frac{2\sqrt{2}}{7}e^{j111°}, \frac{2\sqrt{2}}{7}e^{j249°}, \frac{2\sqrt{2}}{7}e^{j111°}, \frac{2\sqrt{2}}{7}e^{j111°}\right)$$

This transform approach to m-sequences is not popular in the literature. As is evident from Lemma 2.5, this gives a generalised approach to m-sequence-type correlation sequences. Non-binary sequences have also been incorporated in the general results of designing generalised cyclic sequences with desired ideal and near ideal correlations.

This auto-correlation property is useful for many applications as mentioned in the first chapter. For instance, in Radar Ranging, a long m-sequence (depending upon the maximum range to be estimated) is transmitted. The received sequence is a delayed version of the original, delay being directly proportional to the range of the target. This is correlated with a replica of the original and time-shifts counted till a peak is obtained. This gives an estimate of the target range. Another potential use is in the identification of linear cyclic-shift invariant (LCSIV) systems.

2.3 LCSIV SYSTEMS



Let $\underline{\underline{Z}}$ be an N-point LCSIV system. Then,

$$\left.\begin{aligned} w_i &= \sum_{j=0}^{N-1} z_{i-j}\, x_j \\ &= \sum_{j=0}^{N-1} z_j\, x_{i-j} \end{aligned}\right\}, (i-j) \bmod N. \qquad (2.20)$$

Alternatively, $\underline{w} = \underline{\underline{Z}}\ \underline{x}$; where $\underline{\underline{Z}} = (z_{ij})_{N \times N}$,

$$z_{ij} = z_{i-j} ,\ (i-j) \bmod N.$$

Rows of $\underline{\underline{Z}}$ are cyclic shifts of each other.

For instance, for N = 4

$$\begin{bmatrix} x_o \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} z_o & z_3 & z_2 & z_1 \\ z_1 & z_o & z_3 & z_2 \\ z_2 & z_1 & z_o & z_3 \\ z_3 & z_2 & z_1 & z_o \end{bmatrix} \begin{bmatrix} w_o \\ w_1 \\ w_2 \\ w_3 \end{bmatrix}$$

2.3.1 Elementary Properties of LCSIV Systems

PROPERTY 1: DFT row and column vectors form an eigensignal set for LCSIV systems.

PROOF: Consider $\underline{\underline{Y}} = \underline{\underline{F}}\ \underline{\underline{Z}}\ \underline{\underline{F}}^{-1}$, where $\underline{\underline{F}}$ is the N x N DFT matrix.

$$\underline{\underline{F}}\ \underline{\underline{F}}^{*} = N\ \underline{\underline{I}}$$

So, $\underline{\underline{Y}} = \frac{1}{N}\ \underline{\underline{F}}\ \underline{\underline{Z}}\ \underline{\underline{F}}^{*}$

Let $\underline{\underline{G}} = \underline{\underline{Z}}\ \underline{\underline{F}}^{*}$

So, $g_{ik} = \sum_{m=0}^{N-1} z_{im}\ f^{*}_{mk}$

$$y_{nk} = \frac{1}{N} \sum_{i=0}^{N-1} f_{ni}\ g_{ik}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} f_{ni} \sum_{m=0}^{N-1} z_{im}\ f^{*}_{mk}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} f_{ni}\ f^{*}_{mk}\ z_{im}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} f_{ni}\ f^{*}_{mk}\ z_{i-m}\ (f^{*}_{nm}\ f_{nm}),\ (f^{*}_{nm}\ f_{nm}=1 \text{ and } z_{im} = z_{i-m})$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} f_{n,(i-m)}\ z_{i-m}\ f^{*}_{m,(k-n)}$$

$$= \frac{1}{N} \sum_{m=0}^{N-1} f^*_{m,(k-n)} \sum_{i=0}^{N-1} f_{n,(i-m)} \; z_{i-m}$$

Let i-m = s, then,

$$y_{nk} = \frac{1}{N} \sum_{m=0}^{N-1} f^*_{m,(k-n)} \sum_{s=0}^{N-1} f_{ns} \; z_s$$

$$= Z_n \sum_{m=0}^{N-1} f^*_{m,(k-n)} \; , \; (Z_n = \sum_{s=0}^{N-1} f_{ns} \; z_s)$$

$\underline{Z}$ is the DFT of $(z_o z_1 \ldots z_{N-1})^T$.

$$\text{Thus, } y_{nk} = \begin{cases} N \; Z_n & , \; n=k \\ 0 & , \; n \neq k \end{cases}$$

Therefore, $\frac{1}{N} \underline{\underline{Y}}$ is a diagonal matrix with diagonal entries as the DFT values of the LCSIV system vector $\underline{z}$. The similarity transformation $\underline{\underline{F}} \; \underline{\underline{Z}} \; \underline{\underline{F}}^{-1}$ uses $\underline{\underline{F}}$ to diagonalize $\underline{\underline{Z}}$. Hence, the rows and columns of $\underline{\underline{F}}$ are eigenvectors of $\underline{\underline{Z}}$.

Q.E.D.

<u>PROPERTY 2</u>: $\underline{w} = N \; \underline{\underline{F}}^* \; (\underline{Z} \cdot \underline{X})$

i.e. the output $\underline{w}$ is N times the inverse DFT of the termwise product of DFTs of the system vector $\underline{z}$ and input $\underline{x}$.

This follows easily from 1.

<u>PROPERTY 3:</u> If $\underline{\underline{Q}}^k$ is the cyclic-shift operator i.e.,

$$\underline{\underline{Q}}^k \; \underline{u}_i = \underline{u}_{i+k} \; , \quad (i+k) \bmod N$$

which is a k-cyclic-shift of sequence $\underline{u}$, the system matrix $\underline{\underline{Z}}$

commutes with $\underline{\underline{O}}^k$.

$$\underline{\underline{Z}}\ \underline{\underline{O}}^k\ \underline{x} = \underline{\underline{O}}^k\ \underline{\underline{Z}}\ \underline{x}$$

This is the cyclic-shift invariant property and follows readily from (2.20).

2.3.2 LCSIV System - Identification Scheme

A simple arrangement for identification of an LCSIV system is shown in Fig. 2.3:

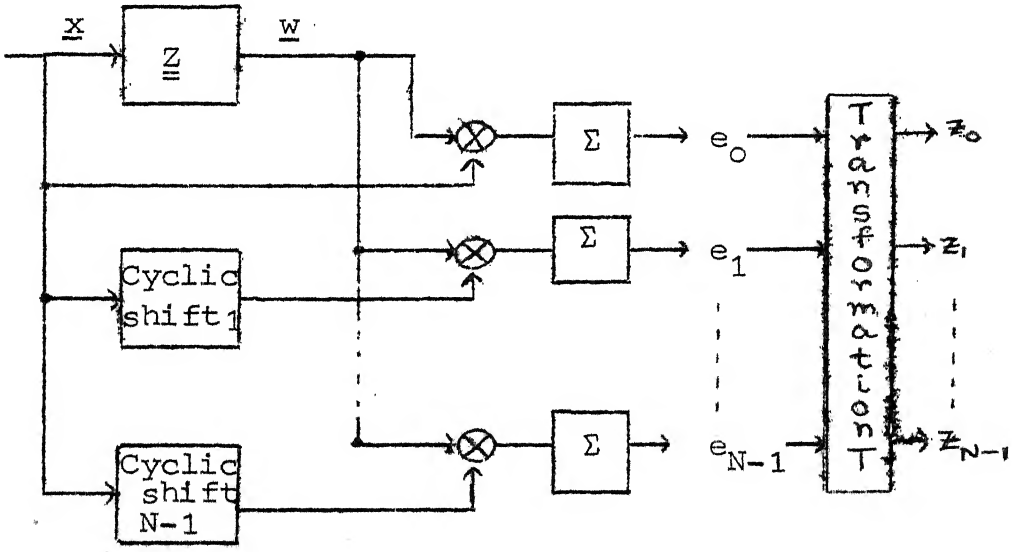


FIG. 2.3

From the figure: $w_i = \sum_j x_{i-j}\, z_j$

$$e_k = \sum_i w_i\, x_{i-k}$$

$$= \sum_i \left(\sum_j x_{i-j}\, z_j \right) x_{i-k}$$

$$= \sum_j z_j \sum_i x_{i-j} x_{i-k}$$

$$= \sum_j z_j p_x (j-k)$$

$\underline{x}$ is the perturbation signal to be chosen to have ideal or near-ideal auto-correlation. Two choices are of interest:

(i) Let $\underline{x}$ be an N-length FZC-sequence

then, $p_x(j-k) = N \delta_{jk}$

So, $e_k = N z_k$, i.e., $z_k = \frac{1}{N} e_k$.

Each e_k is proportional to z_k.

(ii) Choose $\underline{x}$ to be an N-length m-sequence ($N = 2^n-1$)

then, $e_k = N z_k - \sum_{\substack{j \\ j \neq k}} z_j$

In other words,

$$\begin{bmatrix} N & -1 & \cdots & -1 \\ -1 & N & \cdots & -1 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ -1 & -1 & \cdots & N \end{bmatrix} \begin{bmatrix} z_o \\ z_1 \\ \cdot \\ \cdot \\ z_{N-1} \end{bmatrix} = \begin{bmatrix} e_o \\ e_1 \\ \cdot \\ \cdot \\ e_{N-1} \end{bmatrix}$$

Solution of this is:

$$\begin{bmatrix} z_o \\ z_1 \\ \cdot \\ \cdot \\ z_{N-1} \end{bmatrix} = \begin{bmatrix} 2/(N+1) & 1/(N+1) \ldots 1/(N+1) \\ 1/(N+1) & 2/(N+1) \ldots 1/(N+1) \\ \cdot & \cdot \\ \cdot & \cdot \\ 1/(N+1) & 1/(N+1) \ldots 2/(N+1) \end{bmatrix} \begin{bmatrix} e_o \\ e_1 \\ \cdot \\ \cdot \\ e_{N-1} \end{bmatrix}$$

i.e. $z_k = \frac{2}{N+1} e_k + \frac{1}{N+1} \sum_{j \neq k} e_j$

So, $\underline{z} = \underline{\underline{T}}\, \underline{e}$

The interrelation of sequences with good cyclic correlation properties, LCSIV systems and DFT has been presented here as a prelude to a similar study of LDSIV systems and sequences with good dyadic correlation properties. Before we go on to that in the following chapters, we present briefly some sequences with good aperiodic correlation properties.

2.4 SEQUENCES WITH GOOD APERIODIC CORRELATION PROPERTIES

Recent advances in spread-spectrum code-division multiple access (SS-CDMA) communications have focussed attention on the need for large sets of $\{+1, -1\}$-valued sequences having good periodic and aperiodic correlation properties to be used as signatures for various users. A detailed analysis of the requirements for such sequences and important correlation parameters of LFSR and related sequences are presented in [Sarwate and Pursley, 1980] and [Pursley and Roefs, 1979]. Some salient points are presented here.

Aperiodic auto- and cross-correlation of $\underline{u} = (u_o \ldots u_{N-1})$ and $\underline{v} = (v_o \ldots v_{N-1})$ are defined as:

$$C_u(s) = \begin{cases} \sum_{j=s}^{N-1} u_j\, u_{j-s} , & 1-N \leqslant s \leqslant N-1 , \\ 0 , & |s| \geqslant N . \end{cases}$$

$$C_{uv}(s) = \begin{cases} \sum\limits_{i=s}^{N-1} u_j \, v_{j-s} \, , & 0 \leqslant s \leqslant N-1 \\ \sum\limits_{j=s}^{N-1} v_j \, u_{j-s} \, , & 1-N \leqslant s < 0 \\ 0 \, , & |s| \geqslant N \end{cases}$$

Ideal and near-ideal correlations are defined similar to the periodic case.

$\{+1, -1\}$ Barker sequences are known to have good auto-correlation. But they are not known to exist beyond length 13. If u is a Barker sequence then:

$$C_u(s) = \begin{cases} N \, , & s = 0 \\ 0 \, , & s \text{ odd} \\ 1 \, , & s \text{ even} \end{cases}$$

Example 2.5: The length-13 Barker sequence, u and C_u are :

u	1	1	1	1	1	-1	-1	1	1	-1	1	-1	1
$C_u(s)$	13	0	1	0	1	0	1	0	1	0	1	0	1

Generalized Barker sequences have also been studied but are of limited practical value.

Another class of aperiodic sequences is Huffman sequences. If u is such an N-length sequence then:

$$C_u(s) = \begin{cases} C_u(0) \, , & s = 0 \\ 0 \, , & s = 1, \ 2, \ldots, \ (N-2) \\ 1 \, , & s = (N-1) \end{cases}$$

<u>Example 2.6</u>: A length-5 integer Huffman sequence $\underline{u}$ is:

$\underline{u}$	1	2	2	-2	1
$\underline{C}_u$	14	0	0	0	1

But these sequences are non-binary ones and hence not used frequently.

The choice again falls on LFSR and related sequences like Gold and Kasami sequences. These sequences have the near ideal cross-correlation property:

$$\lim_{N \to \infty} \frac{\underline{C}_{C_{max}}}{C(0)} \to 0 .$$

Large sets of these sequences are known as N becomes larger and larger. Hence they are suitable for SS-CDMA systems. Tables of correlation parameters for LFSR, Gold and Kasami sequences upto length 255 (2^8-1) are given in [Pursley and Roefs, 1979].

This brings us to an end of the background material on sequences with good periodic and aperiodic correlation properties. Now we go on to the domain of dyadic correlation and LDSIV systems and analyse a class of Boolean functions for their dyadic correlation properties.

CHAPTER 3

DYADIC CORRELATION AND LDSIV SYSTEMS

This chapter deals with dyadic correlation, LDSIV systems and their relation to Walsh-Hadamard transform (WHT). After presenting dyadic correlation and its relation to LDSIV systems, in Section 3.1, we review Walsh-Hadamard transform in Section 3.2. Elementary properties of dyadic correlation and LDSIV systems in terms of WHT are expounded in Section 3.3. Section 3.4 gives a scheme for identification of LDSIV systems using dyadic correlation and sequences with ideal dyadic auto-correlation property. A typical hardware realisation of a 64-bit dyadic correlator constitutes Section 3.5. Finally, Section 3.6 presents briefly the WHT-based classification of Boolean functions, which is to prove useful in dyadic correlation analysis of NRQFs in the next chapter.

3.1 DYADIC CORRELATION

Dyadic correlation, $\underline{b}_{uv}$, between two N-point $(N=2^n)$ sequences,

$\underline{u} = (u_o u_1 \ldots u_{N-1})$ and

$\underline{v} = (v_o v_1 \ldots v_{N-1})$ is defined as:

$$b_{uv}(s) = \sum_{i=0}^{N-1} u_i v_{i\ominus s} \quad , \; s = 0,\; 1, \ldots, (N-1).$$

$$= \sum_{i=0}^{N-1} u_i v_{i\oplus s} \qquad (3.1)$$

where $i = (i_n \; i_{n-1} \ldots \; i_1)$, $s = (s_n \; s_{n-1} \ldots \; s_1)$ are the binary representations of i and s,

$i\ominus s = (i_n \ominus s_n \; i_{n-1} \ominus s_{n-1} \; \ldots\ldots \; i_1 \ominus s_1)$,

$i\oplus s = (i_n \oplus s_n \; i_{n-1} \oplus s_{n-1} \; \ldots\ldots \; i_1 \oplus s_1)$ are the bitwise mod 2 difference and sum of i and s; $\ominus$ and $\oplus$ are same mod 2.

In terms of the dyadic matrix, $\underline{\underline{V}}$,

$$\underline{b}_{uv} = \underline{\underline{V}} \; \underline{u}, \text{ where } v_{ij} = v_{i\oplus j} \; , \; \underline{u} = (u_o u_1 \ldots u_{N-1})^T.$$

<u>Example 3.1</u>: Let $\underline{u} = (u_o u_1 u_2 u_3)$ and $\underline{v} = (v_o v_1 v_2 v_3)$ be two 4-length sequences.

$$\underline{b}_{uv} = \begin{bmatrix} b_o \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} v_o & v_1 & v_2 & v_3 \\ v_1 & v_o & v_3 & v_2 \\ v_2 & v_3 & v_o & v_1 \\ v_3 & v_2 & v_1 & v_o \end{bmatrix} \begin{bmatrix} u_o \\ u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

Similar to the cyclic case, ideal dyadic auto-correlation for an N-length sequence is defined as:

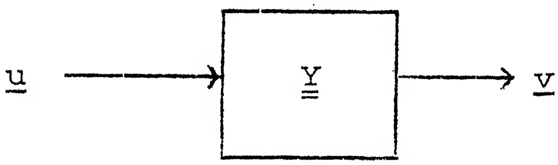
$$b_u(s) = N \, \delta_{so} \quad , \; s=0,1,\ldots,(N-1) \qquad (3.2)$$

Ideal cross-correlation is:

$$b_{uv}(s) = 0 \qquad , \; s=0,1,\ldots,(N-1) \qquad (3.3)$$

Sequences with such properties are to be discussed later.

Dyadic correlation, which is shown to be the same as dyadic convolution, relates the output to the input of linear dyadic-shift invariant (LDSIV) systems. These systems are characterised by dyadic matrices. If $\underline{\underline{Y}}$ is an N x N $(N=2^n)$ LDSIV system, then,



$$v_i = \sum_{j=0}^{N-1} y_{i\ominus j}\, u_j \qquad \text{(CONVOLUTION)}$$

$$= \sum_{j=0}^{N-1} y_{j\ominus i}\, u_j \qquad \text{(CORRELATION)}$$

$$= \sum_{j=0}^{N-1} y_{i\oplus j}\, u_j$$

Alternatively, $\underline{v} = \underline{\underline{Y}}\, \underline{u}$, where $\underline{\underline{Y}} = (y_{ij})_{N \times N}$, $y_{ij} = y_{i\oplus j}$

Hence, properties of LDSIV systems are nothing but those of the operator $\underline{\underline{Y}}$ which also defines dyadic correlation.

Various aspects of dyadic correlation and LDSIV systems can be studied using Walsh-Hadamard transform which is reviewed here briefly.

3.2 WALSH-HADAMARD TRANSFORM

The Walsh-Hadamard Transform (WHT) [Ahmed and Rao, 1975] of an $N = 2^n$-point signal represents its sequency-content or the

Walsh functions' content among the first N i.e. 0 to N-1 Walsh functions. Each row of the transform matrix is an N-point Walsh function. This is similar to the frequency-spectrum, represented by the Fourier transform, of a signal. WHT can be defined with respect to the following three different orderings of the Walsh-functions in the transform matrix:

(1) Sequency-Ordered Transform

Rows of this transform matrix, $\underline{\underline{W}}$, are Walsh-functions in ascending order of their number of zero-crossings i.e. the sequency. The ith row $\underline{W}_i$ is the Walsh function with i zero-crossings. For an N-point ($N=2^n$) signal, $\underline{x}$, this transform, $\underline{X}_W$, is:

$\underline{X}_W = \frac{1}{N}\,\underline{\underline{W}}\,\underline{x}$, where $\underline{W}$ is the N x N sequency-ordered transform matrix defined below:

$$w_{ij} = (-1)^{\sum_{k=0}^{n-1} (i_{n-k} \oplus i_{n-k-1}) j_k} \tag{3.4}$$

where i and j have the binary representation:

$$i = (i_{n-1}\, i_{n-2} \,\ldots\ldots\, i_1 i_o),\ i = \sum_{k=0}^{n-1} i_k . 2^k$$

$$j = (j_{n-1}\, j_{n-2} \,\ldots\ldots\, j_1 j_o),\ j = \sum_{k=0}^{n-1} j_k . 2^k,$$

$$i_k, j_k \in \{0,\ 1\} \text{ and } i_n = 0.$$

A few trivial properties of $\underline{\underline{W}}$ are:

(i) $w_{ij} = w_{ji}$ (SYMMETRY) (3.5)

(ii) $w_{ij} \cdot w_{ik} = w_{i,j\oplus k}$ (CLOSURE) (3.6)

(iii) $\sum_{k=0}^{N-1} w_{ik} \, w_{jk} = N \, \delta_{ij}$ (ORTHOGONALITY) (3.7)

or $\underline{\underline{W}} \cdot \underline{\underline{W}} = N \, \underline{\underline{I}}$

or $\underline{\underline{W}}^{-1} = \frac{1}{N} \underline{\underline{W}}$ (3.8)

So, $\underline{x} = \underline{\underline{W}} \, \underline{X}_W$.

<u>Example 3.2</u>: The 4 x 4 matrix $\underline{\underline{W}}$ with its sequency ordering is:

$$\underline{\underline{W}} = \begin{array}{c c c} & & \text{Sequency} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} & \begin{array}{c} \underline{W}_o \\ \underline{W}_1 \\ \underline{W}_2 \\ \underline{W}_3 \end{array} & \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} \end{array}$$

(2) <u>Paley-Ordered Transform</u>

The transform matrix $\underline{\underline{P}}$ results in the transform:

$$\underline{X}_P = \frac{1}{N} \underline{\underline{P}} \, \underline{x} \, ,$$

where $$p_{ij} = (-1)^{\sum_{k=0}^{n-1} i_{n-k-1} \, j_k} \qquad (3.9)$$

A comparison of (3.4) and (3.9) shows that if

$t = (t_{n-1} \, t_{n-2} \ldots t_1 t_o)$ such that $t_s = i_{s+1} \oplus i_s$, $s=0, 1, \ldots (n-1)$

then $\underline{W}_i = \underline{P}_t$.

But t is the Gray code of i denoted by i_G.

Thus, $\underline{W}_i = \underline{P}_{i_G}$

Conversely, $i_s = t_s \oplus i_{s+1}$ for the given t; s=0,1,...(n-1).

This is the reversed Gray code, ${}^{r}t_G$, of t.

Thus, $\underline{P}_t = \underline{W}_{{}^{r}t_G}$.

<u>Example 3.3</u>: For N = 4,

$$\underline{\underline{P}} = \begin{array}{c} \\ \left[\begin{array}{rrrr} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right] \end{array} \begin{array}{ccccc} & i & & {}^{r}i_G & \\ \underline{P}_o & 0=00 & & 00=0 & \underline{W}_o \\ \underline{P}_1 & 1=01 & & 01=1 & \underline{W}_1 \\ \underline{P}_2 & 2=10 & & 11=3 & \underline{W}_3 \\ \underline{P}_3 & 3=11 & & 10=2 & \underline{W}_2 \end{array}$$

$\underline{\underline{P}}$ also satisfies the properties (3.5), (3.6), (3.7) and (3.8).

(3) <u>Hadamard-Ordered Transform</u>

This transform matrix, $\underline{\underline{H}}$, has properties similar to $\underline{\underline{W}}$ and $\underline{\underline{P}}$,

$$\underline{X}_H = \frac{1}{N}\,\underline{\underline{H}}\,\underline{x}\ , \text{ where } h_{ij} = (-1)^{\langle i,j\rangle} \tag{3.10}$$

$$= (-1)^{\sum_{k=0}^{n-1} i_k j_k} ,$$

$\langle i,j\rangle$ is the inner product mod 2 of i and j.

Comparing (3.9) and (3.10), it is seen that if $i_R = (i_o i_1 \ldots i_{n-1})$, the bit-reversed i, then,

$$\underline{H}_i = \underline{P}_{i_R} \text{ and } \underline{P}_i = \underline{H}_{i_R} ,$$

Example 3.4: For N = 4 ,

$$\underline{\underline{H}} = \begin{array}{c} \\ \left[\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right] \end{array} \begin{array}{cccc} & \underline{i} & \underline{i_R} & \\ \underline{H}_o & 00 & 00 & \underline{P}_o \\ \underline{H}_1 & 01 & 10 & \underline{P}_2 \\ \underline{H}_2 & 10 & 01 & \underline{P}_1 \\ \underline{H}_3 & 11 & 11 & \underline{P}_3 \end{array}$$

Rows and columns of each of the transform matrices are linear Boolean functions (LBFs) to be defined at a later point in this chapter. In addition, rows of $\underline{\underline{H}}$ are in terms of the inner product of indices which is a natural representation for LBFs. This property of Hadamard-ordered transform has been used throughout this work.

Having dealt with the preliminaries of various transforms, we pass on to an analysis of dyadic correlation and LDSIV systems using the Hadamard transform.

3.3 ELEMENTARY PROPERTIES OF DYADIC CORRELATION AND LDSIV SYSTEMS

PROPERTY 1: EIGENSIGNALS

N-point Walsh functions are the eigensignals of LDSIV systems, i.e. the rows and columns of Walsh matrices are eigenvectors of dyadic matrices.

PROOF: Consider $\underline{\underline{G}} = \underline{\underline{H}}\ \underline{\underline{Y}}\ \underline{\underline{H}}^{-1}$, where $\underline{\underline{H}}$ is the N x N Hadamard matrix and $\underline{\underline{Y}}$ is the system matrix.

$$\underline{\underline{G}} = \frac{1}{N}\, \underline{\underline{H}}\; \underline{\underline{Y}}\; \underline{\underline{H}} \quad (\text{as } \underline{\underline{H}}^{-1} = \frac{1}{N}\, \underline{\underline{H}})$$

$$g_{nk} = \frac{1}{N} \sum_{i=0}^{N-1} h_{ni} \sum_{m=0}^{N-1} y_{im}\, h_{mk}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} y_{im}\, h_{ni}\, h_{mk}$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} y_{im}\, h_{ni}\, h_{mk}\, (h_{nm}\, h_{nm}), \quad (h_{nm}^{2} = 1)$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} h_{n,i\oplus m}\, y_{i\oplus m}\, h_{m,n\oplus k}, \quad (y_{im} = y_{i\oplus m} \text{ and CLOSURE property of } \underline{\underline{H}}).$$

$$= \frac{1}{N} \sum_{m=0}^{N-1} h_{m,n\oplus k} \sum_{i=0}^{N-1} h_{n,i\oplus m}\, y_{i\oplus m}$$

Let $i\oplus m = s$, then,

$$g_{nk} = \frac{1}{N} \sum_{m=0}^{N-1} h_{m,n\oplus k} \sum_{s=0}^{N-1} h_{ns}\, y_s$$

$$= \sum_{m=0}^{N-1} h_{m,n\oplus k}\, Y_n ,$$

where Y_n is the nth Hadamard coefficient of $\underline{y}$ as $\underline{Y} = \frac{1}{N}\, \underline{\underline{H}}\, \underline{y}$,

$\underline{y} = (y_o y_1 \cdots y_{N-1})^T$ is the system sample vector.

Thus, $g_{nk} = Y_n \sum_{m=0}^{N-1} h_{m,n\oplus k}$

Now $\sum_{m=0}^{N-1} h_{m,n\oplus k} = N\delta_{nk}$, because sum of any row or column entries of an $\underline{\underline{H}}$ matrix is zero except the zeroth row and column.

So, $g_{nk} = N\, Y_n\, \delta_{nk}$.

$$\text{or} \quad \frac{1}{N}\underline{\underline{G}} = \begin{bmatrix} Y_o & 0 & \cdots & \cdots & 0 \\ 0 & Y_1 & 0 & \cdots & 0 \\ \cdot & & & & \\ \cdot & & & & \\ 0 & 0 & 0 & \cdots & Y_{N-1} \end{bmatrix}$$

$\frac{1}{N}\underline{\underline{G}}$ is a diagonal matrix with the diagonal entries as the WHT-values of the system vector $\underline{y}$. We have been able to diagonalize $\underline{\underline{Y}}$ using the similarity transformation $\underline{\underline{H}}\,\underline{\underline{Y}}\,\underline{\underline{H}}^{-1}$. Hence, the rows and columns of $\underline{\underline{H}}$ are eigenvectors of $\underline{\underline{Y}}$.

Q.E.D.

<u>Example 3.5</u>: Let $\underline{\underline{Y}}$ be a 4 x 4 LDSIV system matrix. Choosing the third row of $\underline{\underline{H}}$, $\underline{H}_3$, we get

$$\underline{\underline{Y}}\,\underline{H}_3^T = \begin{bmatrix} y_o & y_1 & y_2 & y_3 \\ y_1 & y_o & y_3 & y_2 \\ y_2 & y_3 & y_o & y_1 \\ y_3 & y_2 & y_1 & y_o \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = (y_o-y_1-y_2+y_3) \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$$

So, $\underline{H}_3$ is one of the eigenvectors with the eigenvalue $(y_o-y_1-y_2+y_3)$. Also, as a verification:

$$\underline{\underline{H}}\,\underline{\underline{Y}}\,\underline{\underline{H}}^{-1} = \begin{bmatrix} y_o+y_1+y_2+y_3 & 0 & 0 & 0 \\ 0 & y_o-y_1+y_2-y_3 & 0 & 0 \\ 0 & 0 & y_o+y_1-y_2-y_3 & 0 \\ 0 & 0 & 0 & y_o-y_1-y_2+y_3 \end{bmatrix}$$

The ith diagonal entry is the ith Hadamard coefficient of $\underline{y} = (y_0 y_1 y_2 y_3)^T$.

PROPERTY 2: DYADIC-SHIFT INVARIANT PROPERTY

If $\underline{\underline{R}}^k$ is the dyadic shift operator such that $\underline{\underline{R}}^k\ \underline{u}_i = \underline{u}_{i\oplus k}$ which is the kth dyadic shift of $\underline{u}$, then the dyadic correlation operator, $\underline{\underline{Y}}$, commutes with $\underline{\underline{R}}^k$,

$$\underline{\underline{Y}}\ \underline{\underline{R}}^k\ \underline{u} = \underline{\underline{R}}^k\ \underline{\underline{Y}}\ \underline{u}\ .$$

PROOF: $\qquad \underline{v} = \underline{\underline{Y}}\ \underline{u}$

Let $\quad {}^s\underline{v} = \underline{\underline{Y}}\ \underline{\underline{R}}^k\ \underline{u}$

$$\text{Thus,}\quad {}^s v_i = \sum_{j=0}^{N-1} y_{ij}\ u_{j\oplus k}$$

Let $j\oplus k = t$, so, $j = t\oplus k$.

$$\text{Thus,}\quad {}^s v_i = \sum_{t=0}^{N-1} y_{i\oplus t\oplus k}\ u_t\ ,\quad (y_{ij} = y_{i\oplus j})$$

$$= (\underline{\underline{R}}^k\ \underline{\underline{Y}}\ u)_i$$

Hence, $\underline{\underline{Y}}\ \underline{\underline{R}}^k\ \underline{u} = \underline{\underline{R}}^k\ \underline{\underline{Y}}\ \underline{u}$

Q.E.D.

PROPERTY 3: TRANSFORM REPRESENTATION OF DYADIC CORRELATION

The dyadic correlation, $\underline{v}$, between $\underline{u}$ and $\underline{y}$ is N times the inverse WHT of the product of WHTs, $\underline{U}$ and $\underline{Y}$, of $\underline{u}$ and $\underline{y}$.

i.e. $\underline{v} = N\ \underline{\underline{H}}\left(\underline{Y.U}\right)$, $\underline{U} = \frac{1}{N}\ \underline{\underline{H}}\ \underline{u}$,

$$\underline{Y} = \frac{1}{N}\ \underline{\underline{H}}\ \underline{y}\ .$$

PROOF: $$v_i = \sum_{j=0}^{N-1} y_{i\oplus j}\, u_j$$

$$\text{Let } \underline{V} = \frac{1}{N}\, \underline{\underline{H}}\, \underline{v} .$$

$$\text{Thus, } V_t = \frac{1}{N} \sum_{i=0}^{N-1} h_{ti}\, v_i$$

$$= \frac{1}{N} \sum_{i=0}^{N-1} h_{ti} \sum_{j=0}^{N-1} y_{i\oplus j}\, u_j$$

$$\text{Let } i \oplus j = k .$$

$$\text{Thus, } V_t = \frac{1}{N} \sum_{k=0}^{N-1} h_{t,k\oplus j} \sum_{j=0}^{N-1} y_k\, u_j$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} h_{tk}\, y_k \sum_{j=0}^{N-1} h_{tj}\, u_j ,$$

$$= \frac{N^2}{N} \cdot \frac{1}{N} \sum_{k=0}^{N-1} h_{tk}\, y_k \cdot \frac{1}{N} \sum_{j=0}^{N-1} h_{tj}\, u_j$$

$$= N \cdot Y_t \cdot U_t$$

$$\text{So, } \underline{V} = N(\underline{Y}.\underline{U})$$

$$\text{Hence, } \underline{v} = N\underline{\underline{H}}\ (\underline{Y}.\underline{U})$$

Q.E.D.

This property is evident from property 1. As Walsh functions form the eigensignal set for $\underline{\underline{Y}}$, so the input-output of an LDSIV system are related through the WHT similar to LTIV systems where sinusoids are the eigensignals and, accordingly, Fourier transform relates the input-output.

Now we go on to demonstrate the use of ideal dyadic autocorrelation sequences in the identification of LDSIV systems.

3.4 IDENTIFICATION OF LDSIV SYSTEMS

A block schematic for this purpose is shown in Fig. 3.1.

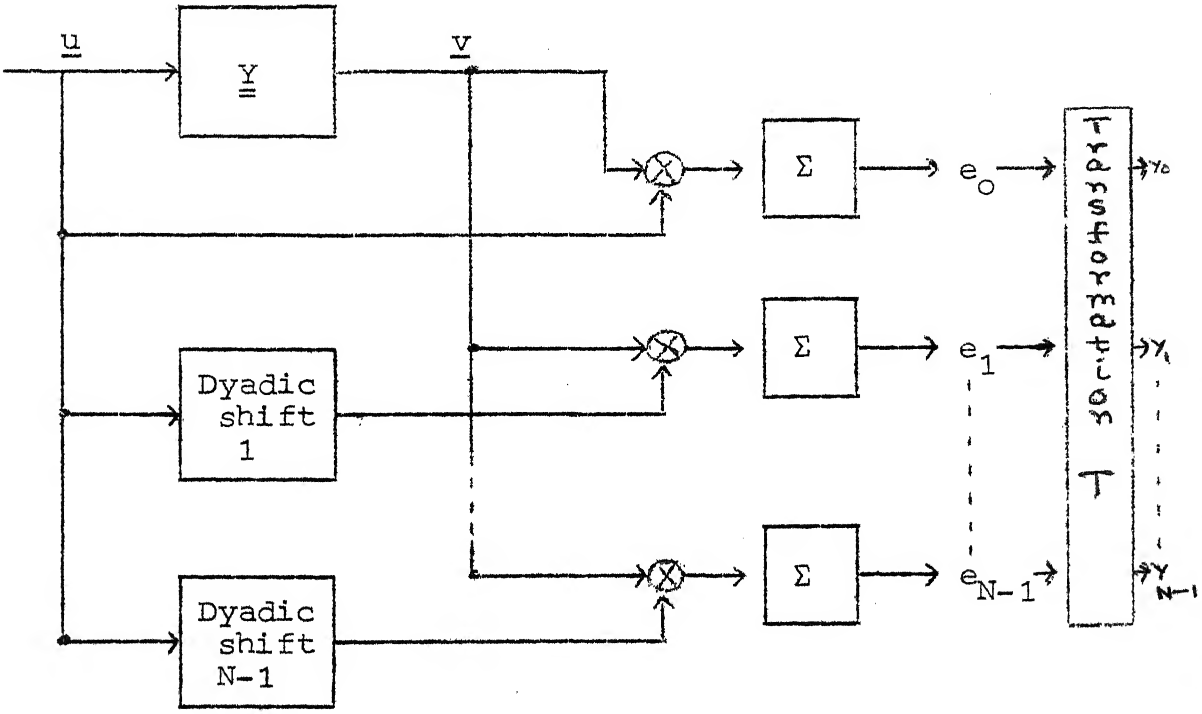


FIG. 3.1

It follows that:
$$v_i = \sum_j u_{i\oplus j}\, y_j$$

$$\begin{aligned} e_k &= \sum_i v_i\, u_{i\oplus k} \\ &= \sum_i \Big(\sum_j u_{i\oplus j}\, y_j \Big)\, u_{i\oplus k} \\ &= \sum_j y_j \sum_i u_{i\oplus j}\, u_{i\oplus k} \\ &= \sum_j y_j\, b_u(j\oplus k) \end{aligned}$$

So, if the perturbation signal $\underline{u}$ is chosen to be such that,

$$b_u(s) = N \delta_{so} \text{ , then}$$

$$e_k = N y_k$$

Thus, $y_k = \frac{1}{N} e_k$

In terms of the transformation $\underline{\underline{T}}$,

$$\begin{bmatrix} y_o \\ y_1 \\ \cdot \\ \cdot \\ y_{N-1} \end{bmatrix} \begin{bmatrix} 1/N & 0 & \cdots\cdots\cdots & 0 \\ 0 & 1/N & 0 \cdots\cdots & 0 \\ \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 \cdots\cdots & 1/N \end{bmatrix} \begin{bmatrix} e_o \\ e_1 \\ \cdot \\ \cdot \\ e_{N-1} \end{bmatrix}$$

Hence, all components of $\underline{y}$ are completely known.

The identification requires a dyadic correlator. A typical circuit realization of a 64-bit dyadic correlator is presented next.

3.5 THE DYADIC CORRELATOR

Dyadic correlation between two $N = 2^n$-point functions $\underline{f}$ and $\underline{g}$ can be implemented in two ways:

(i) Computationally using the fast Walsh-Hadamard Transform (FWHT) [Ahmed and Rao, 1975].

$$\underline{b}_{fg} = 2^n \underline{\underline{H}} (\underline{F} \cdot \underline{G}), \; \underline{F} = \frac{1}{N} \underline{\underline{H}} \, \underline{f}, \; \underline{G} = \frac{1}{N} \underline{\underline{H}} \, \underline{g}$$

$\underline{F}$, $\underline{G}$ & $\underline{\underline{H}}$ ($\underline{F}.\underline{G}$) can be implemented using the FWHT very efficiently.

(ii) Using digital hardware to implement the hard-wired correlator. This uses the definition:

$$b_{fg}(s) = \sum_{x=0}^{N-1} (-1)^{f(x)\oplus g(x\oplus s)}$$

$$= \text{(Number of zeros in } f(x)\oplus g(x\oplus s)) - \text{(number of ones in } f(x)\oplus g(x\oplus s))$$

A typical circuit for 2^6-point functions using 16-1 MUXES, shift-registers and counters is shown in Fig. 3.2.

The correlator consists of a PRE-SET REGISTER which contains $s = (s_5 s_4 \ldots s_0)$, the dyadic shift for which the correlation is desired. These bits are X-ORED with the output of a mod-64 counter counting from 0 thru 63 to give the six control bits c_o to c_5 for the MUXES. c_5 and c_4 control the 1-4 DEMUX whose outputs are the strobe inputs of the 4 16-1 MUXES. $ST_i=0$ means the MUX is disabled and $ST_i=1$ enables the MUX. ST_i along with c_3 to c_0 connect the output of the suitable MUX to $g(x\oplus s)$ as x goes from 0 thru 63. Each $g(x\oplus s)$ is XOR-ed successively with f_o to f_{63}. This output governs the count of a 7-bit up-down counter pre-set at 63. A '0' counts up and a '1' counts down. Hence, the output of the counter after 64 clock pulses is the difference between number of zeros and ones of $(g(x\oplus s) + f(x))$plus the preset number 63. Subtracting 63 out of it gives the dyadic correlation $b_{fg}(s)$.

Similarly, correlator for any 2^n-point functions can be realized.

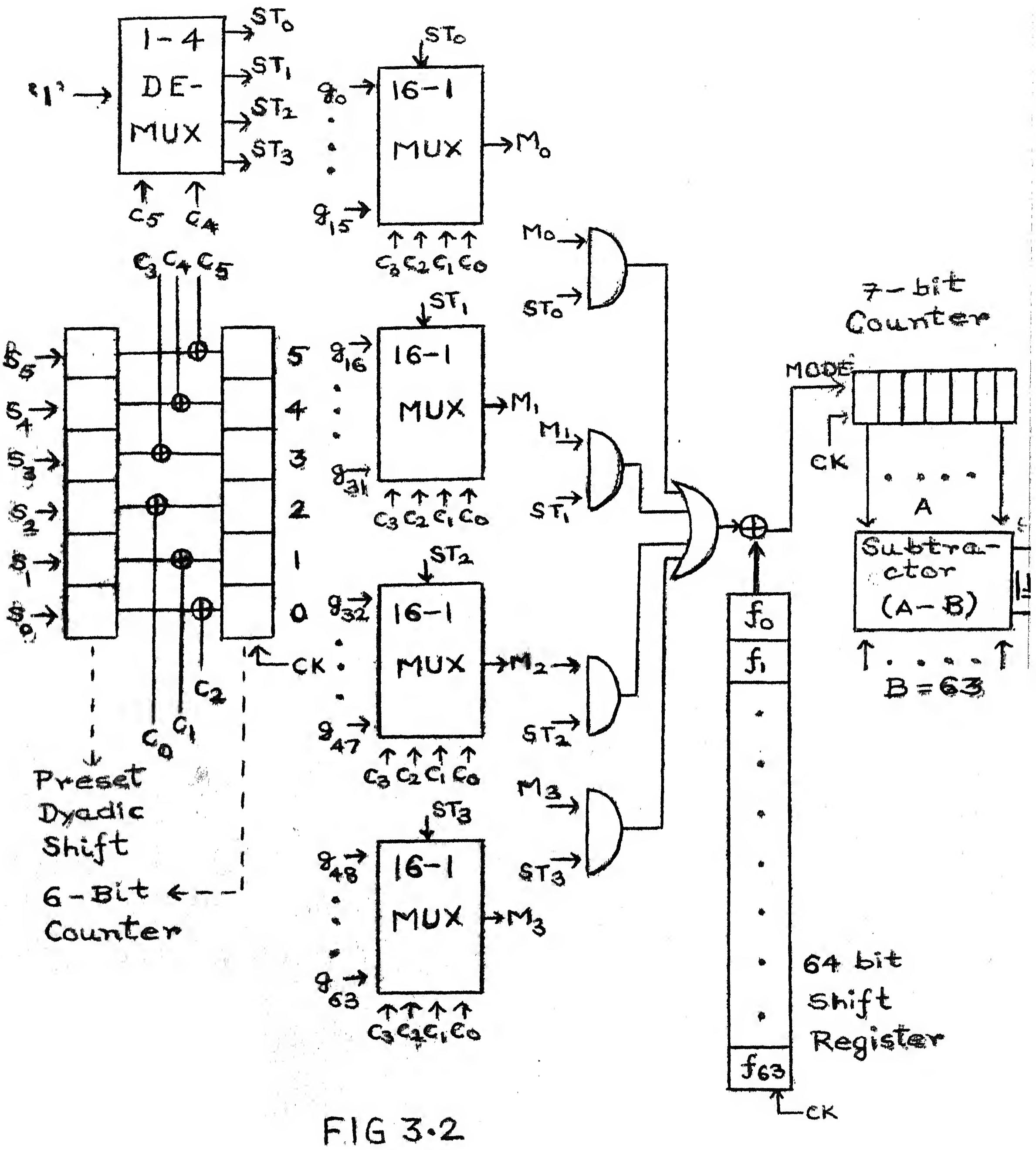

'1'
1-4 DE-MUX
ST0
ST1
ST2
ST3
C5
C4
g0
g15
16-1 MUX
M0
C3 C2 C1 C0
g16
g31
M1
ST1
g32
g47
M2
ST2
g48
g63
M3
ST3
C3 C4 C5
S5
S4
S3
S2
S1
S0
5
4
3
2
1
0
CK
C2
C0
C1
Preset Dyadic Shift
6-Bit Counter
M0
ST0
M1
ST1
M2
ST2
M3
ST3
7-bit Counter
MODE
CK
A
Subtractor (A-B)
B = 63
f0
f1
f63
64 bit Shift Register
CK

FIG 3.2

Now, WHT-based classification of binary Boolean functions is briefly dealt with as it will be of use in dyadic correlation analysis later.

3.6 NOTE ON THE CLASSIFICATION OF BOOLEAN FUNCTIONS

Boolean functions can be divided into various equivalence classes in terms of their Walsh-Hadamard Transforms [Karpovsky, 1976]. As mentioned earlier, each row of $\underline{\underline{H}}$, $\underline{H}_i$, is the ith linear binary Boolean function in the $\{1, -1\}$ -form. The cth linear Boolean function of n-variables in $\{0, 1\}$-form is defined as:

$$\oplus_f^{(c)}(x) = \sum_{i=0}^{n-1} c_i \; x_i \qquad (3.11)$$

where $c = (c_{n-1} \; c_{n-2} \; \ldots\ldots \; c_o)$,

$x = (x_{n-1} \; x_{n-2} \; \ldots\ldots \; x_o)$; x_i, $c_i \in \{0,1\}$; $x=0, 1, \ldots, (2^n-1)$.

Also, $\oplus_f^{(c)}(x) = \langle c, x \rangle$

Its $\{1, -1\}$ - form is:

$$\oplus_f^{(c)}(x) = (-1)^{\oplus_f^{(c)}(x)} = (-1)^{\langle c, x\rangle}$$

Now, $\underline{H}_i = \{ h_{ij} \; , \; j = 0, \; 1, \; \ldots, \; (2^n-1)\}$

Each $h_{ij} = (-1)^{\langle i, j\rangle}$

So, as j varies from 0 to 2^n-1,

$\underline{H}_i = \oplus_f^{(i)}(x)$, the ith LBF.

For any N(2^n)-point Boolean function $\underline{g}$,

$$\underline{G} = \frac{1}{N} \underline{\underline{H}}\ \underline{g}$$

$$G_i = \frac{1}{N} \sum_{j=0}^{N-1} h_{ij}\ g_j\ ,\ i = 0,\ 1, \ldots,\ (N-1).$$

Thus, each G_i is the normalised correlation between the ith LBF in $\{1, -1\}$ -form and $\underline{g}$. It also gives the distance between $\underline{g}$ and the ith LBF. These $\underline{G}$'s can be used to classify Boolean functions.

Example 3.6: Consider the classification of LBFs themselves. LBFs will be classified both in their $\{0, 1\}$ and $\{1, -1\}$ forms.

The ith LBF can be written as:

$$\oplus_{\underline{f}}(i) = \frac{1}{2} (\underline{H}_o - \underline{H}_i) \tag{3.12}$$

So, $$\oplus_{\underline{F}}(i) = \frac{1}{N}\ \underline{\underline{H}}\ .\ \oplus_{\underline{f}}(i)$$

$$\oplus_{F_j}(i) = \frac{1}{N} \langle \underline{H}_j\ ,\ \oplus_{\underline{f}}(i) \rangle$$

$$= \frac{1}{N} \cdot \frac{1}{2} (\langle \underline{H}_j\ ,\ \underline{H}_o \rangle - \langle \underline{H}_j\ ,\ \underline{H}_i \rangle)$$

$$= \frac{1}{2N} (N\ \delta_{jo} - N\ \delta_{ji})$$

$$= \frac{1}{2} (\delta_{jo} - \delta_{ji})$$

Hence, WHT of the ith-LBF is:

$$\oplus_{F_j}(i) = \begin{cases} 1/2 & , j = 0 \\ -1/2 & , j = i \\ 0 & , j \neq 0\ ,\ i\ ;\ j = 1,\ 2, \ldots,\ (N-1) \end{cases} \tag{3.13}$$

This can be expressed as:

Lemma 3.1:

A binary function $\underline{f}$ in the $\{0, 1\}$ -form is an LBF iff:

$$F_j = \begin{cases} 1/2 & , j = 0 \\ -1/2 & , \text{for some } j = k \\ 0 & , j \neq 0, k , \end{cases}$$

where $\underline{F} = \frac{1}{N} \underline{\underline{H}} \, \underline{f}$.

Then it is the kth LBF.

Example 3.7: Consider the 3-variable 7th-LBF,

$$\oplus_{f}^{(7)} (x) = x_o \oplus x_1 \oplus x_2, \ k = (111) = 7.$$

x	000	001	010	011	100	101	110	111
$\oplus_{\underline{f}}^{(7)}$	0	1	1	0	1	0	0	1
$\oplus_{\underline{F}}^{(7)}$	1/2	0	0	0	0	0	0	-1/2

Classification of LBFs in the $\{+1, -1\}$ form is even more evident. The ith LBF is:

$$\oplus_{\underline{\hat{f}}}^{(i)} = \underline{H}_i$$

So, $$\oplus_{\hat{F}_j}^{(i)} = \frac{1}{N} \langle \underline{H}_j , \underline{H}_i \rangle \quad ; \langle \underline{H}_j , \underline{H}_i \rangle = \sum_{t=0}^{N-1} (\underline{H}_j \cdot \underline{H}_i)_t$$

$$= \frac{1}{N} \cdot N \, \delta_{ji}$$

$$= \delta_{ji}$$

Thus, $$\oplus_{\hat{F}_j}^{(i)} = \begin{cases} 1 , & j = i \\ 0 , & \text{otherwise} \end{cases} \qquad (3.14)$$

Lemma 3.2:

A binary function $\underline{f}$ in the $\{+1, -1\}$-form is the kth LBF iff:

$$F_j = \begin{cases} 1 , & j = k \\ 0 , & \text{otherwise.} \end{cases}$$

Example 3.8: Another class of $\{+1, -1\}$ functions called Bent functions are classified with respect to their WHT.

A $\{+1, -1\}$ $\underline{f}$ is a Bent function of n variables iff;

$$F_j = \pm \frac{1}{2^{n/2}} , \quad j = 0, 1, \ldots, 2^n - 1.$$

$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4$ is one of the bent functions of four variables.

This brings to an end the exposition of WHT techniques and their application to correlation analysis. Now we go on to use these for a detailed dyadic correlation analysis of non-repetitive quadratic forms.

CHAPTER 4

NON-REPETITIVE QUADRATIC FORMS

This chapter is devoted to an analysis of dyadic correlation and related properties of non-repetitive quadratic forms (NRQFs). In Section 4.1 we define NRQFs and give some preliminary details about them - viz. principal NRQFs (p-NRQFs), special NRQF (s-NRQF), elementary properties, generation of NRQFs using counters and minimal LFSR circuits. Walsh-Hadamard transforms of NRQFs are computed in Section 4.2. In Section 4.3 these are used to derive dyadic auto-correlation of NRQFs. Their cross-correlation properties are expounded in Section 4.4 using permutation cycle structure relationships between them. Section 4.5 gives the number of NRQFs related through L-length permutation cycles. Finally, some results on periodic and aperiodic correlation parameters of p-NRQFs of 4,6 and 8 variables are presented in Section 4.6.

4.1 DEFINITION

Non-repetitive quadratic forms (NRQFs) are a special class of degree 2 binary Boolean functions. They are defined for an even number of variables. An NRQF f(x) of $n = 2s$ variables can be expressed as a polynomial in the following way [Karpovsky, 1976]:

$$f(x) = \sum_{\substack{i \neq j \\ i,j}}^{\oplus} (x_i)^{a_i} (x_j)^{a_j} \qquad (4.1)$$

$$\text{where} \quad x = \sum_{i=1}^{n} x_i \, 2^{i-1} ,$$

$x = (x_{2s} \, x_{2s-1} \cdots x_1)$ is the binary representation of x,

$i, j \in \{1, 2, \ldots\ldots, 2s\}$; $a_i, a_j, x_i, x_j \in \{0, 1\}$,

$$(x_i)^{a_i} = \begin{cases} x_i & \text{if } a_i = 1 \\ \overline{x_i} & \text{if } a_i = 0 \end{cases}$$

Each x_i occurs exactly once and each term is a quadratic term, hence, the name non-repetitive quadratic forms. $\sum^{\oplus}$ is the exclusive - OR addition operation.

4.1.1 Principal NRQFs

If a_i and a_j are 1 for all $i, j \in \{1, 2, \ldots, n\}$ in (4.1), then the resulting NRQF is:

$$f(x) = \sum_{\substack{i \neq j \\ i,j}}^{\oplus} x_i \, x_j \, .$$

Such NRQFs with none of the variables complemented are called Principal NRQFs (p-NRQFs).

Example 4.1: For $n = 4$ variables, a principal NRQF is

$$f(x) = x_1 x_2 \oplus x_3 x_4 \, ,$$

and $g(x) = \bar{x}_1x_4 \oplus \bar{x}_2\bar{x}_3$ is a non-principal NRQF (np-NRQF). Both are tabulated in Table 4.1:

Table 4.1

x	$(x_4$	x_3	x_2	$x_1)$	f(x)	g(x)
0	0	0	0	0	0	1
1	0	0	0	1	0	1
2	0	0	1	0	0	0
3	0	0	1	1	1	0
4	0	1	0	0	0	0
5	0	1	0	1	0	0
6	0	1	1	0	0	0
7	0	1	1	1	1	0
8	1	0	0	0	0	0
9	1	0	0	1	0	1
10	1	0	1	0	0	1
11	1	0	1	1	1	0
12	1	1	0	0	1	1
13	1	1	0	1	1	0
14	1	1	1	0	1	1
15	1	1	1	1	0	0

Lemma 4.1:

Each principal form is related to the other by a permutation of variables.

Hence, the principal forms are an equivalence class of NRQFs with permutation of variables as the group operation. Permutations of variables can be represented using cycle structures or binary permutation matrices.

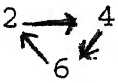
Example 4.2: Consider the two principal NRQFs:

$$f_1(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \text{ and}$$

$$f_2(x) = x_1x_6 \oplus x_3x_2 \oplus x_5x_4$$

$f_2(x)$ is a permutation of $f_1(x)$, cycle structure being:

$$(1)(2\ 4\ 6)(3)(5)$$

This means that x_1, x_3, x_5 are unchanged whereas x_4 is replaced by x_2, x_6 by x_4 and x_2 by x_6 or 

Alternatively,

$$f_2(x) = f_1(x\,\underline{\underline{A}}),\quad x = (x_1x_2x_3x_4x_5x_6)$$

where the permutation matrix is:

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence, two n variable principal NRQFs f(x) and g(x) are related through the invertible linear transformation:

$f(x) = g(x\,\underline{\underline{A}})$, where $\underline{\underline{A}}$ is an n xn permutation matrix.

Lemma 4.2:

Each non-principal NRQF is some dyadic shifted version of its respective principal NRQF.

A non-principal NRQF g(x) of n variables and its principal NRQF f(x) are related as:

$$g(x_n x_{n-1} \cdots x_1) = f((x_n)^{a_n} (x_{n-1})^{a_{n-1}} \cdots (x_1)^{a_1}) ,$$

where $a = (a_n a_{n-1} \cdots a_1)$ and

$$a_i = \begin{cases} 0 \text{ , if } x_i \text{ is complemented in } g(x) \\ 1 \text{ , otherwise} \end{cases}$$

In other words, $g(x) = f(x \oplus a)$ which is nothing but the ath dyadic shift of f(x).

In vector notation,

$$g(\underline{x}) = f(\underline{x} \oplus \underline{a}) \text{ where } \underline{a} \text{ is a binary n-tuple.}$$

Example 4.3: Consider the p-NRQF of $n = 4$ variables,

$$f(x) = x_1 x_2 \oplus x_3 x_4$$

It generates $2^4 = 16$ NRQFs which are its dyadic shifts for $a = 0, 1, \ldots, 15$. Fifteen of these are np-NRQFs. All of these in their polynomial as well as array form are given in Table 4.2.

Lemmas 4.1 and 4.2 can be combined in:

Lemma 4.3:

Any two n-variable NRQFs, f(x) and g(x) are related through the following transformation of input variables:

Table 4.2

A p-NRQF AND ITS DYADIC SHIFTS

$f(x) = x_1x_2 \oplus x_3x_4$

		x																f(x)
a	$(a_4a_3a_2a_1)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	0 0 0 0	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	$x_1x_2 \oplus x_3x_4$
1	0 0 0 1	0	0	1	0	0	0	1	0	0	0	1	0	1	1	0	1	$\bar{x}_1x_2 \oplus x_3x_4$
2	0 0 1 0	0	1	0	0	0	1	0	0	0	1	0	0	1	0	1	1	$x_1\bar{x}_2 \oplus x_3x_4$
3	0 0 1 1	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	$\bar{x}_1\bar{x}_2 \oplus x_3x_4$
4	0 1 0 0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1	$x_1x_2 \oplus \bar{x}_3x_4$
5	0 1 0 1	0	0	1	0	0	0	1	0	1	1	0	1	0	0	1	0	$\bar{x}_1x_2 \oplus \bar{x}_3x_4$
6	0 1 1 0	0	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0	$x_1\bar{x}_2 \oplus \bar{x}_3x_4$
7	0 1 1 1	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0	$\bar{x}_1\bar{x}_2 \oplus \bar{x}_3x_4$
8	1 0 0 0	0	0	0	1	1	1	1	0	0	0	0	1	0	0	0	1	$x_1x_2 \oplus x_3\bar{x}_4$
9	1 0 0 1	0	0	1	0	1	1	0	1	0	0	1	0	0	0	1	0	$\bar{x}_1x_2 \oplus x_3\bar{x}_4$
10	1 0 1 0	0	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0	$x_1\bar{x}_2 \oplus x_3\bar{x}_4$
11	1 0 1 1	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0	$\bar{x}_1\bar{x}_2 \oplus x_3\bar{x}_4$
12	1 1 0 0	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	$x_1x_2 \oplus \bar{x}_3\bar{x}_4$
13	1 1 0 1	1	1	0	1	0	0	1	0	0	0	1	0	0	0	1	0	$\bar{x}_1x_2 \oplus \bar{x}_3\bar{x}_4$
14	1 1 1 0	1	0	1	1	0	1	0	0	0	1	0	0	0	1	0	0	$x_1\bar{x}_2 \oplus \bar{x}_3\bar{x}_4$
15	1 1 1 1	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	$\bar{x}_1\bar{x}_2 \oplus \bar{x}_3\bar{x}_4$

$$g(\underline{x}) = f(\underline{x}\ \underline{\underline{A}} \oplus \underline{a}) ,$$

where $\underline{\underline{A}}$ is an n x n binary invertible permutation matrix and $\underline{a}$ is a 1 x n binary vector.

Example 4.4: The two NRQFs

$f(x) = x_1x_2 \oplus x_3x_4$ and $g(x) = \bar{x}_1x_4 \oplus \bar{x}_2\bar{x}_3$ are related as:

$g(x) = f(\underline{x}\ \underline{\underline{A}} \oplus \underline{a})$, where $\underline{x} = (x_1x_2x_3x_4)$

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad a = (1 \quad 1 \quad 1 \quad 0)$$

The transformation of this Lemma just rearranges the 0's and 1's of the function to which it is applied without altering their number.

4.1.2 A Special NRQF:

A special NRQF (s-NRQF) [Karpovsky, 1976] amongst the set of p-NRQFs of n = 2t variables is:

$$f^s(x) = \sum_{i=1}^{t} x_i x_{i+t} \qquad (4.2)$$

$$= x_1x_{t+1} \oplus x_2x_{t+2} \oplus \ldots \oplus x_tx_{2t}$$

$f^s(x)$ can also be represented in terms of the t x t Paley-Ordered Matrix $\underline{\underline{P}}$:

$$f^s(x) = \tfrac{1}{2}\,(1 - p_{\overleftarrow{r(x)},e(x)}) \;,$$

where $x = (x_{2t}, \ldots, x_{t+1}, x_t, \ldots. x_1)$,

$\overleftarrow{r(x)} = (x_1, x_2, \ldots, x_t)$ is the bit-reversed form of $r(x)$, the right-half of x;

$r(x) = (x_t, x_{t-1}, \ldots, x_1)$,

$e(x) = (x_{2t}, x_{2t-1}, \ldots, x_{t+1})$ is the lef-half of x,

and $p_{\overleftarrow{r(x)},e(x)}$ is the $(\overleftarrow{r(x)}, e(x))$-th entry of $\underline{\underline{P}}$.

Example 4.5: For $n = 4$ variables,

$$\begin{aligned} f^s(x) &= x_1x_3 \oplus x_2x_4 \\ &= \tfrac{1}{2}(1 - p_{(x_1x_2),(x_4x_3)}) \end{aligned}$$

$f^s(x)$ calculated using both these definitions is presented in Table 4.3.

All other NRQFs can be obtained from the s-NRQF using the transformation of Lemma 4.3.

4.1.3 Elementary Properties of NRQFs

PROPERTY 1: $f^s(x) = 0$ for $0 \leqslant x \leqslant 2^t$, $n = 2t$ variables.

PROPERTY 2: If $f(x)$ is an NRQF of $n = 2s$ variables. Then, the number of ones in $f(x) = 2^{2s-1} - 2^{s-1}$ and number of zeros $= 2^{2s-1} + 2^{s-1}$.

PROPERTY 3: Let $N(n = 2s)$ be the number of p-NRQFs of n variables.

Table 4.3

SPECIAL NRQF OF 4 VARIABLES

$$f^S(x) = x_1x_3 \oplus x_2x_4$$

x	$(x_4x_3x_2x_1)$	$x_1 \cdot x_3$	$x_2 \cdot x_4$	$f^S(x)$	$\overleftarrow{\hat{r}(x)}$	$e(x)$	$\frac{1}{2}(1-p_{\overleftarrow{r(x)},e(x)})$
0	0 0 0 0	0	0	0	00=0	00=0	0
1	0 0 0 1	0	0	0	10=2	00=0	0
2	0 0 1 0	0	0	0	01=1	00=0	0
3	0 0 1 1	0	0	0	11=3	00=0	0
4	0 1 0 0	0	0	0	00=0	01=1	0
5	0 1 0 1	1	0	1	10=2	01=1	1
6	0 1 1 0	0	0	0	01=1	01=1	0
7	0 1 1 1	1	0	1	11=3	01=1	1
8	1 0 0 0	0	0	0	00=0	10=2	0
9	1 0 0 1	0	0	0	10=2	10=2	0
10	1 0 1 0	0	1	1	01=1	10=2	1
11	1 0 1 1	0	1	1	11=3	10=2	1
12	1 1 0 0	0	0	0	00=0	11=3	0
13	1 1 0 1	1	0	1	10=2	11=3	1
14	1 1 1 0	0	1	1	01=1	11=3	1
15	1 1 1 1	1	1	0	11=3	11=3	0

$$\underline{\underline{P}}\ 4x\ 4 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 2 & 1 & -1 & 1 & -1 \\ 3 & 1 & -1 & -1 & 1 \end{array}$$

Then $N(2s) = (2s-1).N(2s-2)$

$$= \frac{(2s-1)!}{(2)^{s-1}\ (s-1)!} \tag{4.3}$$

Each p-NRQF generates $(2^{2s}-1)$ np-NRQFs.

Thus, total number of NRQFs of 2s variables

$$= \frac{(2)^{s+1}\ (2s-1)!}{(s-1)!} \tag{4.4}$$

4.1.4 Generation of NRQFs

An NRQF of $n = 2s$ variables is generated by a combinatorial circuit of ANDs and EXORs getting its inputs from a mod-2^n counter.

Number of AND gates required = s.

Number of EXOR gates needed = s-1.

Example 4.6: A typical circuit to generate

$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ is shown in Fig. 4.1.

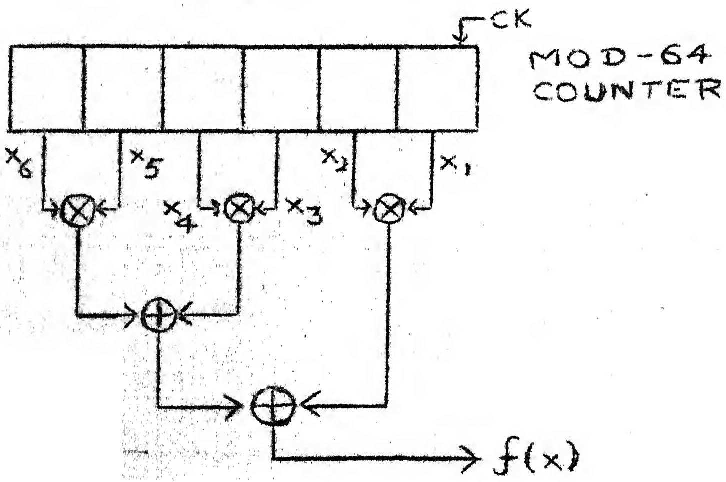


FIG. 4.1

Complexity of an N-length sequence vis-a-vis maximal-length sequence is guaged in terms of the number of stages of a minimal LFSR circuit needed to generate it. This follows from the fact that only 2r terms of an r-stage LFSR-generated m-sequence are sufficient to know it completely. For an arbitrary sequence, longer is the minimal LFSR, greater is the number of terms necessary to decipher it completely and hence, more complex is it with respect to the same length m-sequence. Following this definition of complexity for NRQFs also, number of stages (r) of minimal LFSR to generate p-NRQFs of 2, 4, 6 and 8 variables have been computed. Massey's shift-register synthesis algorithm [Massey, 1969] is used. The p-NRQFs and their respective r's are presented in Table 4.4. The notation adopted to represent p-NRQFs is that only their indices are given e.g. $f(x) = x_1x_2\oplus x_3x_4\oplus x_5x_7\oplus x_6x_8$ is written as 12 34 57 68.

Table 4.4

n	p-NRQF	r
2	12	4
4	12 34	9
	13 24	10
	14 23	9

n	p-NRQF	r	n	p-NRQF	r
6	12 34 56	36	6	12 35 46	37
	12 36 45	33		13 24 56	38
	13 25 46	35		13 26 45	30
	14 23 56	39		14 25 36	36
	14 26 35	35		15 34 26	34
	15 32 46	34		15 36 24	37
	16 34 52	34		16 35 24	34
	16 32 45	34			

n	p-NRQF	r	n	p-NRQF	r
8	12 34 56 78	144	8	12 34 57 68	148
	12 34 58 76	132		12 35 46 78	152
	12 35 47 78	140		12 35 48 67	124
	12 36 54 78	156		12 36 57 48	133
	12 36 58 47	141		12 37 56 48	133
	12 37 54 68	136		12 37 58 46	141
	12 38 56 74	129		12 38 57 64	129
	12 38 54 67	129		13 24 56 78	144
	13 24 57 68	150		13 24 58 76	134
	13 25 46 78	152		13 25 47 68	142
	13 25 48 67	126		13 26 54 78	158
	13 26 57 48	131		13 26 58 47	139
	13 27 56 48	131		13 27 54 68	136
	13 27 58 46	139		13 28 56 74	131
	13 28 57 64	131		13 28 54 67	131
	14 32 56 78	144		14 32 57 68	151
	14 32 58 76	135		14 35 26 78	158
	14 35 27 78	140		14 35 28 67	131
	14 36 52 78	156		14 36 57 28	131
	14 36 58 27	135		14 37 56 28	131
	14 37 52 68	142		14 37 58 26	135
	14 38 56 72	132		14 38 57 62	133
	14 38 52 67	133		15 34 26 78	158
	15 34 27 68	143		15 34 28 76	131
	15 32 46 78	152		15 32 47 68	143
	15 32 48 67	127		15 36 24 78	156
	15 36 27 48	137		15 36 28 47	131
	15 37 26 48	136		15 37 24 68	143
	15 37 28 46	131		15 38 26 74	133
	15 38 27 64	132		15 38 24 67	133
	16 34 52 78	159		16 34 57 28	131

...contd.

n	p-NRQF	r	n	p-NRQF	r
8	16 34 58 72	132	8	16 35 42 78	159
	16 35 47 28	131		16 35 48 27	137
	16 32 54 78	159		16 32 57 48	130
	16 32 58 47	138		16 37 52 48	136
	16 37 54 28	131		16 37 58 42	134
	16 38 52 74	133		16 38 57 24	133
	16 38 54 27	132		17 34 56 28	130
	17 34 52 68	142		17 34 58 26	132
	17 35 46 28	130		17 35 42 68	140
	17 35 48 62	137		17 36 54 28	130
	17 36 52 48	137		17 36 58 42	134
	17 32 56 48	130		17 32 54 68	136
	17 32 58 46	138		17 38 56 24	133
	17 38 52 64	133		17 38 54 62	133
	18 34 56 72	130		18 34 57 62	130
	18 34 52 76	130		18 35 46 72	130
	18 35 47 62	130		18 35 42 67	130
	18 36 54 72	130		18 36 57 42	130
	18 36 52 47	130		18 37 56 42	130
	18 37 54 62	130		18 37 52 46	130
	18 32 56 74	130		18 32 57 64	130
	18 32 54 67	130			

As expected from the non-linearity of NRQFs, they are considerably more complex than the same length m-sequences. A rough estimate of the complexity ratio from the given data is that the ratio is greater than $\frac{2^n/2}{n}$ i.e., $\frac{2^{n-1}}{n}$.

With these preliminaries on NRQFs, we pass on to finding their WHT.

4.2 WALSH-HADAMARD TRANSFORM OF NRQFs

This part is devoted to finding the WHT of NRQFs in general and will be useful in their correlation analysis. From now onwards, NRQFs will be taken in their converted $\{+1, -1\}$ form using the transformation:

$$c_{f(x)} = (-1)^{f(x)}$$

For the WHT analysis, only p-NRQFs have been considered because the WHTs of np-NRQFs follow directly from their respective p-NRQFs as follows:

Let f(k) be a p-NRQF of n variables and g(k) be the np-NRQF which is an sth dyadic shift of f(k):

$$\text{So,} \quad g(k) = f(k \oplus s)$$

$$G_i = \sum_{k=0}^{2^n-1} h_{ik} \, c_{g(k)}$$

$$= \sum_{k=0}^{N-1} h_{ik} \, c_{f(k \oplus s)}; \quad N = 2^n$$

$$\langle i,k\rangle = i_n k_n \oplus i_{n-1} k_{n-1} \oplus \dots \oplus i_1 k_1$$

$$= \sum_{t=1}^{n} i_t k_t$$

$\langle i,k\rangle$ is the ith LBF as pointed out in the last section.

Substituting for $\langle i,k\rangle$ and f(k), their polynomial representations, we get

$$F_i = \sum_{k=0}^{N-1} (-1)^{\sum_{t=1}^{n} i_t k_t \oplus \sum_{\substack{m\neq j\\ m,j}} k_m k_j}$$

$t,\ m,\ j \in \{1,\ 2, \dots\dots,\ n\}$

It is inferred that F_i is the difference between the number of zeros and ones in the composite function $C_i(k)$ formed by the mod 2 sum of the ith LBF and the NRQF.

$$C_i(k) = \sum_{t=1}^{n} i_t k_t \oplus \sum_{\substack{m\neq j\\ m,j}} k_m k_j$$

So, to know F_i, the number of ones and zeros in $C_i(k)$ should be known. Each $C_i(k)$ is formed out of an LBF from the linear vector space of LBFs of n variables as i varies from 0 to N-1. Three representative cases of i are considered and the rest are shown to be combinations of these.

Case 1: i=0

Case 2: Only one i_t, for $t=1,2,\dots,n$ is one and the rest are zeros.

Case 3: Two of the i_t's $(t=1,2,\dots,n)$, say i_p and i_q are ones and $k_p k_q$ is a quadratic term of the NRQF f(k).

Case 1: $i = 0$

$$F_o = \sum_{k=0}^{N-1} (-1)^{f(k)}$$

$= $ (number of zeros in $f(k)$) $-$ (number of ones in $f(k)$)

$= (2^{2s-1} + 2^{s-1}) - (2^{2s-1} - 2^{s-1})$, (from PROP. 2 of NRQFs)

$= 2^s$.

So, $F_o = 2^s$ (4.5)

Case 2: Only one i_t , for $t = 1, 2, \ldots, n$ is one and the rest are zeros.

Say, $i = \begin{pmatrix} i_n & i_{n-1} & \cdots i_{p+1} & i_p & i_{p-1} \cdots i_1 \\ 0 & 0 & \ldots 0 & 1 & 0 \quad \ldots 0 \end{pmatrix}$, i.e. only $i_p = 1$.

or, $i = 2^{p-1}$.

$$\text{So, } C_i(k) = \bigoplus_{t=1}^{n} i_t k_t \oplus \bigoplus_{\substack{m \neq j \\ m, j}} k_m k_j$$

$$= k_p \oplus \bigoplus_{\substack{m \neq j \\ m, j}} k_m k_j$$

The NRQF $f(k)$ contains exactly one quadratic term, say $k_p k_q$, containing k_p.

$$\text{Thus, } C_i(k) = k_p \oplus k_p k_q \oplus \bigoplus_{\substack{m \neq j \\ m, j \neq p, q}} k_m k_j$$

$$= k_p \bar{k}_q \oplus \bigoplus_{\substack{m \neq j \\ m, j \neq p, q}} k_m k_j$$

$$= f(k_n, k_{n-1}, \ldots, \bar{k}_q, \ldots k_1)$$

This function is nothing but a dyadic shift of f(k), say f(k⊕a) where

$$\begin{array}{lcccccccc} & a_n & a_{n-1} & \ldots a_{q+1} & a_q & a_{q-1} & \ldots a_1 \\ a = (& 0 & 0 & \ldots 0 & 1 & 0 & \ldots 0) \end{array}$$

$$= 2^{q-1}$$

So, $C_i(k) = f(k \oplus a)$

Thus, $C_i(k)$ is also an NRQF.

So, for this case too

$$F_i = 2^s \; ; \quad i = 2^{p-1}, \; p = 1, 2, \ldots, n \tag{4.6}$$

Similar is the case when more than one $i_t = 1$, $t = 1, 2, \ldots, n$, and each k_t for which $i_t = 1$ belongs to a different quadratic term of the NRQF f(k), i.e. at most one component k_t of each quadratic term forms the ith LBF.

If $i_{t_1}, i_{t_2}, \ldots, i_{t_b}$ are ones and the rest zeros, where $t_1, t_2, \ldots t_b \in \{1, 2, \ldots, n\}$ then $k_{t_1}, k_{t_2}, \ldots k_{t_b}$ should belong to different quadratic terms. If such is the case, then each term of the LBF can be combined with the appropriate quadratic terms as shown before and the resulting $C_i(k)$ is another dyadic shift of f(k).

<u>Example 4.7</u>: Consider the NRQF

$f(k) = k_1k_2 \oplus k_3k_4 \oplus k_5k_6$ of $n = 6$ variables.

For $i = 21 = (010101)$,

$$C_{21}(k) = k_1 \oplus k_3 \oplus k_5 \oplus f(k)$$

$$= k_1 \oplus k_1k_2 \oplus k_3 \oplus k_3k_4 \oplus k_5 \oplus k_5k_6$$

$$= k_1\bar{k}_2 \oplus k_3\bar{k}_4 \oplus k_5\bar{k}_6$$

$$= f(k \oplus (101010))$$

$$= f(k \oplus 42),$$

which is the 42nd dyadic shift of f(k).

Hence, $F_{21} = 2^s = 8$.

Thus, $F_i = 2^s$ for i's of the above type.

Number of such i's can be found out. There are s quadratic terms. So, number of such i's

$$= \binom{s}{2}.2^2 + \binom{s}{3}.2^3 + \ldots + \binom{s}{s}.2^s$$

$$= \sum_{j=2}^{s} \binom{s}{j}.2^j \qquad (4.7)$$

Thus, from (4.6) and (4.7), the total number of i's, for which each term of the ith LBF appears in a different quadratic term is:

$$^2N_i = n + \sum_{j=2}^{s} \binom{s}{j}.2^j \qquad (4.8)$$

For all these i's, $F_i = 2^s$.

<u>Example 4.8</u>: Consider $f(k) = k_1k_2 \oplus k_3k_4$, $n=4$, $s=2$.

Number of case 2 i's, $^2N_i = 4 + \binom{2}{2}.2^2 = 4+4 = 8$.

These i's are:

(a) i's having one '1':

(0001) = 1	(0100) = 4
(0010) = 2	(1000) = 8.

(b) i's having two '1''s:

(0101) = 5	(0110) = 6
(1001) = 9	(1010) = 10

So, for all these i's, $F_i = 2^s = 4$.

These i's can also be enumerated using a graphical representation of an NRQF. Let n vertices of a planar graph, G_f, represent the n variables of NRQF f(k). $v_p v_q$ is an edge of G_f, the graph of f(k), iff $k_p k_q$ is a term of f(k). Hence, any NRQF can be graphed onto a disconnected graph with n vertices and s = n/2 edges, each representing a quadratic term.

Example 4.9: Let $f(k) = k_1 k_3 \oplus k_2 k_4$

G_f is shown in Fig. 4.2(a)

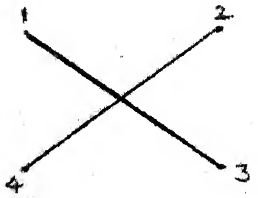
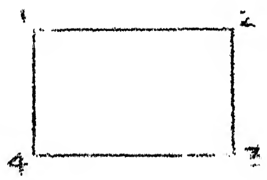


FIG. 4.2(a)

n = 4, No. of edges = 2.

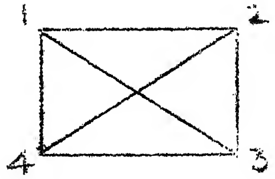
Complement of G_f, ${}^cG_f$, is defined now: ${}^cG_f$ has all possible edges $v_a v_e$ such that $v_a v_e$ is not an edge of G_f, $a, e \in \{1, 2, \ldots, n\}$.

$G_f \cup {}^cG_f$ is the complete graph of n vertices. ${}^cG_f$ and $G_f \cup {}^cG_f$ for the f(k) of the previous example are shown in Figs. 4.2(b) and 4.2(c), respectively.



${}^cG_f$

FIG. 4.2(b)



$G_f \cup {}^cG_f$

FIG. 4.2(c)

A path in a graph G is defined as a sequence of alternating vertices and edges with no vertices repeated. Length of a path with (L+1) vertices is L.

<u>Example 4.10:</u> In the ${}^cG_f$ of Fig. 4.2(b), a 3-length path is:

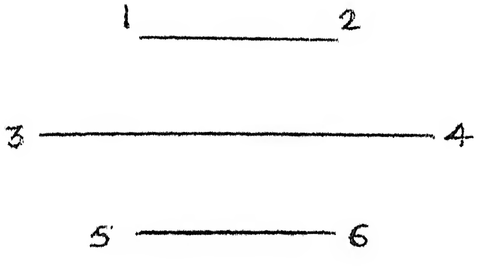
$$\{v_1, v_1v_2, v_2, v_2v_3, v_3, v_3v_4, v_4\}.$$

It can also be represented as $\{v_1, v_2, v_3, v_4\}$.

To enumerate all the i's of case 2, find all L-length paths ($L = 0, 1, 2, \ldots, s-1$) of ${}^cG_f$ which are not permutations of each other and do not include vertices which are adjacent in G_f. Each of these paths represents an i for which $F_i = 2^s$ in accordance with case 2. This will be illustrated with an example.

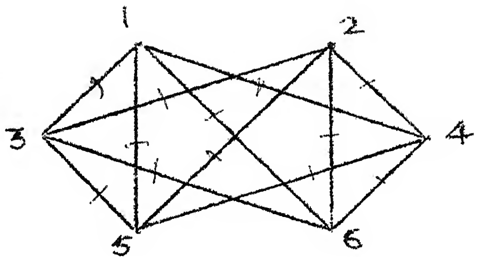
<u>Example 4.11:</u> Let $f(k) = k_1k_2 \oplus k_3k_4 \oplus k_5k_6$, $s = 3$

G_f and ${}^cG_f$ are shown in Figs. 4.2(d) and 4.2(e), respectively.



G_f

FIG. 4.2(d)



^cG_f

FIG. 4.2(e)

For L = 0, 1, 2, the L-length paths and corresponding i's are given in Table 4.5.

Table 4.5

0-length paths	$(i_6i_5i_4i_3i_2i_1)$	i	2-lengths paths	$(i_6i_5i_4i_3i_2i_1)$
$\{k_1\}$	0 0 0 0 0 1	1	$\{k_1, k_3, k_5\}$	0 1 0 1 0 1
$\{k_2\}$	0 0 0 0 1 0	2	$\{k_2, k_3, k_5\}$	0 1 0 1 1 0
$\{k_3\}$	0 0 0 1 0 0	4	$\{k_1, k_4, k_5\}$	0 1 1 0 0 1
$\{k_4\}$	0 0 1 0 0 0	8	$\{k_2, k_4, k_5\}$	0 1 1 0 1 0
$\{k_5\}$	0 1 0 0 0 0	16	$\{k_1, k_3, k_6\}$	1 0 0 1 0 1
$\{k_6\}$	1 0 0 0 0 0	32	$\{k_2, k_3, k_6\}$	1 0 0 1 1 0
(These are all vertices of			$\{k_1, k_4, k_6\}$	1 0 1 0 0 1
^cG_f).			$\{k_2, k_4, k_6\}$	1 0 1 0 1 0
1-Length paths			1-Length paths	
$\{k_1, k_3\}$	0 0 0 1 0 1	5	$\{k_3, k_5\}$	0 1 0 1 0 0
$\{k_2, k_3\}$	0 0 0 1 1 0	6	$\{k_4, k_5\}$	0 1 1 0 0 0
$\{k_1, k_4\}$	0 0 1 0 0 1	9	$\{k_1, k_6\}$	1 0 0 0 0 1
$\{k_1, k_5\}$	0 1 0 0 0 1	17	$\{k_3, k_6\}$	1 0 0 1 0 0
$\{k_2, k_4\}$	0 0 1 0 1 0	10	$\{k_2, k_6\}$	1 0 0 0 1 0
$\{k_2, k_5\}$	0 1 0 0 1 0	18	$\{k_4, k_6\}$	1 0 1 0 0 0

These are edges of ^cG_f

If $k_t \in$ path P, $i_t = 1$, otherwise 0.

$$^2N_i = n + \sum_{j=2}^{s} \left({s \atop j} \right).2^j$$

$$= 6 + \left({3 \atop 2} \right).2^2 + \left({3 \atop 3} \right).2^3$$

$$= 6 + 12 + 8 = 26.$$

There are 6 zero-length paths (these are just the vertices of ^cG_f), 12 one-length paths (edges of ^cG_f) and 8 two-length paths. Hence, the tabulated i's are the case 2 i's for f(k).

<u>Case 3:</u> i is such that only two of the i's (t=1, 2,...,n), say i_p and i_q, are ones and $k_p k_q$ is a quadratic term of the NRQF f(k)

$$\text{Let } i = \begin{array}{cccccccccc} i_n & i_{n-1} & \cdots i_{p+1} & i_p & i_{p-1} & \cdots i_{q+1} & i_q & i_{q-1} & \cdots & i_1 \\ (0 & 0 & \ldots 0 & 1 & 0 & \ldots 0 & 1 & 0 & \ldots & 0) \end{array}$$

$$\text{So } C_i(k) = k_p \oplus k_q \oplus k_p k_q \oplus \sum_{\substack{m \neq j \\ m,j \neq p,q}}^{\oplus} k_j k_m$$

$$= k_p \bar{k}_q \oplus \bar{k}_q \oplus 1 \oplus \sum_{\substack{m \neq j \\ m,j \neq p,q}}^{\oplus} k_j k_m$$

$$= \bar{f}\ (k_n, k_{n-1}, \ldots, \bar{k}_p, \ldots, \bar{k}_q, \ldots, k_1)$$

$$= \bar{k}_q\ \bar{k}_p \oplus \sum_{\substack{m \neq j \\ m,j \neq p,q}}^{\oplus} k_j k_m \oplus 1$$

$$= \bar{f}\ (k \oplus a), \text{ where } a = \begin{array}{ccccccc} a_n & a_{p+1} & a_p & a_{p-1} & \cdots a_q & \cdots & a_1 \\ (0 & \ldots 0 & 1 & 0 & \ldots 1 & \ldots & 0\ ) \end{array}$$

This function is the complement of the ath-dyadic shift of f(k). So, the number of ones and zeros get interchanged vis-a-vis f(k).

So, $F_i = -2^s$ (4.9)

Example 4.12: Let $f(k) = k_1k_2 \oplus k_3k_4$, $n = 4$, $s = 2$.

For $i = 12$ (1100),

$$C_{12}(k) = k_3 \oplus k_4 \oplus k_1k_2 \oplus k_3k_4$$

$$= k_1k_2 \oplus \bar{k}_3\bar{k}_4 \oplus 1$$

So, $F_{12} = -2^2 = -4$.

Cases 3 and 2 can be generalised further to two alternatives:

(a) i is such that the components of an odd number of quadratic terms and single components from any of the other quadratic terms form the LBF. This is similar to (4.9) and hence $F_i = -2^s$.

Example 4.13: Let $f(k) = k_1k_2 \oplus k_3k_4 \oplus k_5k_6 \oplus k_7k_8$,

Consider $i = (11111101) = 253$.

So, $C_{253}(k) = k_1 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8 \oplus f(k)$

$$= \underbrace{k_1 \oplus k_1k_2}_{\text{case 2}} \oplus \underbrace{\sum_{j=3}^{8} k_j \oplus k_3k_4 \oplus k_5k_6 \oplus k_7k_8}_{\text{case 3}}$$

$$= k_1\bar{k}_2 \oplus \bar{k}_3\bar{k}_4 \oplus \bar{k}_5\bar{k}_6 \oplus \bar{k}_7\bar{k}_8 \oplus 1$$

$$= f(k \oplus (11111110)) \oplus 1$$

$$= f(k \oplus 254) \oplus 1$$

Hence, $F_{253} = -2^4 = -16$.

(b) If i is such that the components of an even number of quadratic terms of f(k) and single components from any of the other terms form the LBF, then $F_i = 2^s$.

Example 4.14: Let $f(k) = k_1k_3 \oplus k_2k_4 \oplus k_5k_6$, n=6, s=3

Consider $i = (111110) = 62$

$$\text{So, } C_{62}(k) = k_2 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \oplus f(k)$$

$$= \underbrace{k_3 \oplus k_1k_3}_{\text{case 2}} \oplus \underbrace{k_2 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_2k_4 \oplus k_5k_6}_{\text{case 3}}$$

$$= \bar{k}_1k_3 \oplus \bar{k}_2\bar{k}_4 \oplus \bar{k}_5\bar{k}_6$$

$$= f(k \oplus 59)$$

So, $F_{62} = 2^3 = 8$.

Lemma 4.5:

The unnormalised WHT of an N-point ($N=2^{2s}$) NRQF, f(k), is:

$$F_i = \begin{cases} 2^s & , i = 0 \\ \pm 2^s & , \text{otherwise} \end{cases} \qquad (4.10)$$

Hence, in as much as each F_i is the distance (distance being the correlation) between the ith LBF and the NRQF f(k), every NRQF is equidistant from each element of the set of LBFs.

As an illustration for all the cases, consider an example.

Example 4.15: Let $f(k) = k_1k_2 \oplus k_3k_4$, n=4, s=2

The u-WHT of f(k) alongwith the cases for each i are given in Table 4.6:

Table 4.6

i	$(i_4 i_3 i_2 i_1)$	F_1	Case
0	0 0 0 0	4	1
1	0 0 0 1	4	2
2	0 0 1 0	4	2
3	0 0 1 1	-4	3(a)
4	0 1 0 0	4	2
5	0 1 0 1	4	2
6	0 1 1 0	4	2
7	0 1 1 1	-4	3(a)
8	1 0 0 0	4	2
9	1 0 0 1	4	2
10	1 0 1 0	4	2
11	1 0 1 1	-4	3(a)
12	1 1 0 0	-4	3(a)
13	1 1 0 1	-4	3(a)
14	1 1 1 0	-4	3(a)
15	1 1 1 1	4	3(b)

Functions, which are complements of NRQFs, also have similar u-WHT.

If $g(k) = \overline{f}(k)$,

then $g(k) = 1-f(k)$, ${}^c g(k) = -1.{}^c f(k)$

So, $$G_i = \sum_{k=0}^{N-1} h_{ik} \, {}^c g(k)$$

$$= \sum_{k=0}^{N-1} h_{ik} \, (-f(k))$$

$$= \sum_{k=0}^{N-1} (-1)\ h_{ik}\ f(k)$$

$$= -F_i$$

Hence, $\underline{G} = -\underline{F}$

<u>Lemma 4.6</u>: u-WHT of complement of an NRQF, f(k), is the negative of the u-WHT, $\underline{F}$, of f(k).

An important fact which stands out is that like the FZC sequences of previous chapter which have uniform-magnitude Fourier spectrum, NRQFs have similar Walsh-Hadamard spectrum. Accordingly, it is to be expected that NRQFs have ideal dyadic auto-correlation as the FZC sequences have ideal cyclic auto-correlation. This is demonstrated in the next section.

4.3 DYADIC AUTOCORRELATION OF NRQFs

Dyadic auto-correlation of an $N = 2^n$-point $(n = 2s)$ NRQF f(x), f(x) being taken as ${}^c f(x)$, is:

$$b_f(s) = \sum_{x=0}^{N-1} (-1)^{f(x)} . (-1)^{f(x \oplus s)}$$

$$\text{or } \underline{b}_f = \frac{1}{N}\ \underline{\underline{H}}\ (\underline{F} . \underline{F}) ,$$

where $\underline{F} = \underline{\underline{H}}\ {}^c\underline{f}$ is the u-WHT of ${}^c f(x)$.

Now, $\underline{F} = (2^s \pm 2^s \ldots \pm 2^s)^T$

So, $\underline{F} . \underline{F} = (2^{2s} \ldots\ldots 2^{2s})^T$

$= (N \ldots\ldots N)^T$

Thus, $\underline{b}_f = \frac{1}{N} \underline{\underline{H}} \cdot (N.....N)^T$

$$= \frac{1}{N} \cdot N \cdot \underline{\underline{H}}\, \underline{H}_o \text{ , } \underline{H}_o \text{ is the oth column of } \underline{\underline{H}} \text{ .}$$

$$= (N \quad 0 \; .... \; 0)^T, \quad (\underline{H}_i \; \underline{H}_j^T = N \, \delta_{ij})$$

This is the ideal dyadic auto-correlation. Hence NRQFs are ideal for LDSIV system identification. It is evident that any function having uniform-magnitude WHT spectrum has ideal dyadic auto-correlation. This fact will be further dwelled upon when such functions called bent functions are presented in the next chapter. Presently, we go on to the cross-correlation properties of NRQFs.

4.4 DYADIC CROSS-CORRELATION OF NRQFs:

Dyadic cross-correlation between two n(=2s) variable, N(=2^n)-point NRQFs f(x) and g(x) is defined as:

$$b_{fg}(t) = \sum_{x=0}^{N-1} (-1)^{f(x) \oplus g(x \oplus t)} \tag{4.11}$$

i.e. the t-shift dyadic cross-correlation is the difference in the number of zeros and ones of the composite function, $f(x) \oplus g(x \oplus t)$ - the linear combination of f(x) and t - dyadic shifted g(x).

It is evident that,

$$\underline{b}_{fg} = \underline{b}_{gf}$$

Let $d(x) = f(x \oplus a)$ be the np-NRQF resulting from ath dyadic-shift of its p-NRQF f(x).g(x) be another p-NROF.

Then, $b_{dg}(t) = \sum_{x=0}^{N-1} (-1)^{f(x\oplus a)\oplus g(x\oplus t)}$

Let $x\oplus a = k$

So, $b_{dg}(t) = \sum_{k=0}^{N-1} (-1)^{f(k)\oplus g(k\oplus a\oplus t)}$

$= b_{fg}(a \oplus t)$

This can be stated as:

Lemma 4.7:

Dyadic correlation between ath dyadic shift of a function $f(x)$ and another function $g(x)$ is ath dyadic shift of the dyadic correlation function $b_{fg}(t)$.

This is nothing but dyadic shift invariant property of the correlation operator.

Hence, we need to consider only the principal NRQFs and results for non-principal NRQFs follow in accordance with Lemma 4.7.

In general, two p-NRQFs, $f(x)$ and $g(x)$, are related through permutation of variables as shown in Section 4.1.1. Permutations are represented by their cycle structures. As each variable occurs exactly once in each of the NRQFs, their cycle structure can be established just by inspection.

Example 4.16: Let $f(x) = x_1x_2\oplus x_3x_4\oplus x_5x_6$ (12 34 56)

$g(x) = x_1x_4\oplus x_3x_6\oplus x_5x_2$ (14 36 52) be two p-NRQFs of 6 variables.

(The notation shown in parenthesis is adopted to represent NRQFs).

The cycle structure :

(1)(264)(3)(5)

consists of 3 single-length cycles or identities and 1 three-length cycle. This is called a one 3-length cycle permutation.

Similarly, cycle structure of any two p-NRQFs can be established. We will base our enquiry into cross-correlation of NRQFs on the types of cycle-structures relating them. Firstly, we will find cross-correlation between two NRQFs related through one 2-length cycle. Such permutations are also called Transpositions. All the rest follow easily from these.

4.4.1 Cross-correlation Between Transposition-Related p-NRQFs

Let f(x) and g(x) be two $N=2^n$-point $(n = 2s)$ p-NRQFs related through a transposition. Such NRQFs differ in exactly two of their s quadratic terms.

Example 4.17: Let $f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$

$g(x) = x_1x_3 \oplus x_2x_4 \oplus x_5x_6$

Permutation cycle structure is (1)(23)(4)(5)(6) which is a Transposition.

They differ only in their first two quadratic terms.

From the N-point functions, $f(x)$ and $g(x)$, construct the function $r(x,t)$:

$$r(x,t) = f(x) \oplus g(x \oplus t)$$

So, $b_{fg}(t)$ = (number of zeros in $r(x,t)$) - (number of ones in $r(x,t)$).

In general, $g(x \oplus t)$ can take three different forms according to the value of t as has already been shown in Section 4.2.

(i) $g(x \oplus t) = g(x)$, $t=0$ (case 1 of Sec. 4.2)

(ii) $g(x \oplus t) = g(x) \oplus \sum_{m=1}^{n} c_m x_m$, (case 2 and 3(b) of Sec. 4.2)

$c = (c_n c_{n-1} \ldots c_1)$ and depends on t and $g(x)$.

(iii) $g(x \oplus t) = g(x) \oplus \sum_{m=1}^{n} c_m x_m \oplus 1$ (case 3(a) of Sec. 4.2).

<u>Example 4.18</u>: Consider $g(x) = x_1x_2 \oplus x_3x_4$

(i) Let $t = (0001)$

So, $g(x \oplus t) = \bar{x}_1x_2 \oplus x_3x_4$

$= g(x) \oplus x_2$

Thus, $c = (0010)$ and $\sum_{m=1}^{n} c_m x_m = x_2$ (case 2).

(ii) For $t = (0011)$,

$g(x \oplus t) = \bar{x}_1\bar{x}_2 \oplus x_3x_4$

$= g(x) \oplus x_1 \oplus x_2 \oplus 1$ (case 3(a))

Thus $c = (0011)$, $\sum_m c_m x_m = x_1 \oplus x_2$.

(iii) For $t = (1111)$,

$$g(x \oplus t) = \bar{x}_1 \bar{x}_2 \oplus \bar{x}_3 \bar{x}_4$$

$$= g(x) \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \quad \text{(case 3(b))}$$

Thus, $c = (1111)$, $\sum_m c_m x_m = x_1 \oplus x_2 \oplus x_3 \oplus x_4$

Hence, $r(x,t)$ can take three different forms which are treated separately below.

(A) $r(x,0) = f(x) \oplus g(x)$

(B) $r(x,t) = f(x) \oplus g(x) \oplus \sum_m c_m x_m$

(C) $r(x,t) = f(x) \oplus g(x) \oplus \sum_m c_m x_m \oplus 1$

Case A:

Let the combination of the two quadratic terms in which $f(x)$ and $g(x)$ differ be:

$$x_i x_j \oplus x_k x_q$$

and

$$x_i x_k \oplus x_j x_q ,$$

i.e., the transposition is $(1)(2)\ldots(jk)\ldots(n)$

So, $r(x,0) = f(x) \oplus g(x)$

$$= x_i x_j \oplus x_k x_q \oplus x_i x_k \oplus x_j x_q$$

$$= (x_i \oplus x_q)(x_j \oplus x_k)$$

Let $r_1(x) = x_i \oplus x_q$ and

$r_2(x) = x_j \oplus x_k$ be LBFs of x,

$$x = (x_n \ldots x_i \ldots x_q \ldots x_j \ldots x_k \ldots x_1)$$

assuming $n \geqslant i > q > j > k \geqslant 1$.

So, $r(x,0) = r_1(x)\ r_2(x)$

Number of ones in $r(x,0) = \sum_{x=0}^{N-1} r(x,0)$

$= \sum_{x=0}^{N-1} r_1(x)\ r_2(x)$

$= b_{r_1 r_2}(0)$, the zeroth dyadic correlation between $r_1(x)$ and $r_2(x)$

$\underline{b}_{r_1 r_2} = N\ \underline{\underline{H}}\ (\underline{R}_1 \cdot \underline{R}_2)$, where, $N = 2^{2s}$, $\underline{R}_1 = \frac{1}{N} \underline{\underline{H}}\ \underline{r}_1$,

$\underline{R}_2 = \frac{1}{N} \underline{\underline{H}}\ \underline{r}_2$.

Thus, $b_{r_1, r_2}(0) = 2^{2s} \sum_{m=0}^{N-1} (\underline{R}_1 \cdot \underline{R}_2)_m$.

So, $\underline{R}_1$ and $\underline{R}_2$ have to be found out. As shown in Sec. 3.6, the WHT, $\underline{V}$, of the cth N-point LBF $v(x) = \sum_m c_m x_m$ is:

$$V_m = \begin{cases} \frac{1}{2} & , m = 0 \\ -\frac{1}{2} & , m = c \\ 0 & , \text{otherwise} \end{cases}$$

$$\text{i.e., } \underline{V} = \begin{array}{c} \begin{array}{ccccccccc} 0 & 1 & \ldots\ldots & & c & & \ldots\ldots & N-1 & \end{array} \\ (\frac{1}{2} \quad 0 \ \ldots \ 0 \quad -\frac{1}{2} \quad 0 \ \ldots \ 0 \ )^T \end{array}$$

Now, $r_1(x) = x_i \oplus x_q = \sum_{m=1}^{n} {}^{1}c_m\ x_m$, and $$^1c = (\overset{^1c_n}{0}\ \dots\ \overset{^1c_i}{1}\ \ 0\ \dots\ \overset{^1c_q}{1}\ \ 0\dots\ \overset{^1c_1}{0}) \qquad (4.12)$$

Similarly, $r_2(x) = \sum_{m=1}^{n} {}^2c_m\, x_m$

$$= x_j \oplus x_k\ ,$$

$$^2c = (\overset{^2c_n}{0}\ \dots\ \overset{^2c_j}{1}\ \ 0\ \dots\ \overset{^2c_k}{1}\ \ 0\dots\ \overset{^2c_1}{0}) \qquad (4.13)$$

So, $\underline{R}_1 = (\overset{0}{\tfrac{1}{2}}\ \ \overset{1}{0}\ \dots\ 0\ \ \overset{^1c}{-\tfrac{1}{2}}\ \ 0\ \dots\ \overset{N-1}{0})^T$

and $\underline{R}_2 \quad (\overset{0}{\tfrac{1}{2}}\ \ \overset{1}{0}\ \dots\ 0\ \ \overset{^2c}{-\tfrac{1}{2}}\ \ 0\ \dots\ \overset{N-1}{0})^T$

Thus, $\underline{R}_1 \cdot \underline{R}_2 = (\overset{0}{1/4}\ \ \overset{1}{0}\ \dots\dots\dots\ \overset{N-1}{0})^T$, as $^1c \neq {}^2c$.

So, $\sum_{x=0}^{N-1} r(x,0) = N \sum_{m=0}^{N-1} (\underline{R}_1 \cdot \underline{R}_2)_m$

$$= 2^{2s} . 1/4 = 2^{2s-2}$$

Or , number of ones of $r(x,0) = 2^{2s-2}$.

Number of zeros of $r(x, 0) = 2^{2s} - 2^{2s-2} = 3 . 2^{2s-2}$

Difference $= 3 . 2^{2s-2} - 2^{2s-2} = 2^{2s-1}$

Hence, $b_{fg}(0) = 2^{2s-1}$ (4.14)

i.e., the 0- shift cross-correlation between two transposition-related 2s-variable p-NRQFs is 2^{2s-1}.

Case B: Before we go on to find $b_{fg}(t)$ for this case, we note the relationship between ${}^1c$, ${}^2c$, c and t.

(i) If t is such that $c = {}^1c$, then

$$g(x \oplus t) = g(x) \oplus \sum_m {}^1c_m \, x_m \;, \quad {}^1c \text{ is as in (4.12)}$$

$$= g(x) \oplus x_i \oplus x_q$$

$$= g(x_n \ldots x_i \ldots x_q \ldots \bar{x}_j \ldots \bar{x}_k \ldots x_1), \text{ as } x_i x_k \text{ and } x_j x_q \text{ are terms of } g(x).$$

$$\text{So, } t = (\overset{t_n}{0} \;\ldots\ldots \overset{t_j}{1} \;\; 0 \;\ldots\; \overset{t_k}{1} \;\; 0 \ldots\ldots \overset{t_1}{0})$$

$$= {}^2c \qquad \text{(from 4.13)}.$$

Hence, $t = {}^2c \iff c = {}^1c$ (4.15)

(ii) If t is such that $c = {}^2c$, then

$$g\ (x \oplus t) = g(x) \oplus \sum_m {}^2c_m \, x_m$$

$$= g(x) \oplus x_j \oplus x_k$$

$$= g(x_n \ldots \bar{x}_i \ldots \bar{x}_q \ldots x_j \ldots x_k \ldots x_1)$$

$$\text{So, } t = (\overset{t_n}{0} \;\ldots\ldots \overset{t_i}{1} \;\; 0 \ldots\ldots \overset{t_q}{1} \;\; 0 \ldots\ldots \overset{t_1}{0})$$

$$= {}^1c$$

Thus, $t = {}^1c \iff c = {}^2c$ (4.16)

(iii) If $c = {}^1c \oplus {}^2c = {}^3c$ (say)

$$= (\overset{c_n}{0} \;\ldots\ldots \overset{c_i}{1} \;\; 0 \ldots\ldots \overset{c_q}{1} \;\; 0 \ldots\ldots \overset{c_j}{1} \;\; 0 \ldots\ldots \overset{c_k}{1} \;\; 0 \ldots\ldots \overset{c_1}{0}),$$

$$\text{then} \quad g(x \oplus t) = g(x) \oplus x_i \oplus x_q \oplus x_j \oplus x_k$$

$$= g(x_n \ldots \bar{x}_i \ldots \bar{x}_q \ldots \bar{x}_j \ldots \bar{x}_k \ldots x_1)$$

$$\text{So, } t = (\overset{t_n}{0} \ldots . \overset{t_i}{1} \quad 0 \ldots . \overset{t_q}{1} \quad 0 \ldots . \overset{t_j}{1} \quad 0 \ldots . \overset{t_k}{1} \quad 0 \ldots . \overset{t_1}{0})$$

$$= {}^{s}c$$

$$\text{Thus } t = {}^{3}c \iff c = {}^{3}c \tag{4.17}$$

For all the rest of t's, i.e., for a t such that $c \neq {}^{1}c$, ${}^{2}c$ or ${}^{3}c$, $t \neq {}^{1}c$, ${}^{2}c$ or ${}^{3}c$.

This will help in finding $b_{fg}(t)$ for this case and the next.

For this case,

$$r(x,t) = f(x) \oplus g(x) \oplus \sum_m c_m x_m$$

$$= (x_i \oplus x_q)(x_j \oplus x_k) \oplus \sum_m c_m x_m$$

$$= r_1(x) r_2(x) \oplus r_3(x), \quad r_3(x) = \sum_m c_m x_m$$

$$= r_{1\,2}(x) \oplus r_3(x), \quad r_{1\,2}(x) = r_1(x) r_2(x)$$

$$\sum_{x=0}^{N-1} r(x,t) = \sum_x (r_{12}(x) \oplus r_3(x))$$

$$= \sum_x (r_{12}(x) - r_3(x))^2 \quad \text{(Arithmetic representation of } \oplus\text{).}$$

$$= \sum_x r_{12}(x) + \sum_x r_3(x) - 2 \sum_x r_{12}(x) r_3(x) \tag{4.18}$$

From case A,

$$\sum_x r_{12}(x) = 2^{2s-2} \tag{4.19}$$

$r_3(x)$ is an LBF ,

so $$\sum_x r_3(x) = 2^{2s-1} \qquad (4.20)$$

$$\sum_x r_{12}(x)\, r_3(x) = b_{r_{12}r_3}(0) \qquad (4.21)$$

To find this, we calculate $\underline{R}_{12}$ and $\underline{R}_3$.

(a) $\underline{R}_{12}$:

$$r_1(x) = \sum_{m=1}^{n} {}^1c_m \, x_m$$

So, $\underline{r}_1 = \frac{1}{2}(\underline{H}_0 - \underline{H}_{{}^1c})$ (from 3.15)

Similarly, $r_2(x) = \sum_{m=1}^{n} {}^2c_m \, x_m$

So, $\underline{r}_2 = \frac{1}{2}(\underline{H}_0 - \underline{H}_{{}^2c})$

$$\underline{r}_{12} = \underline{r}_1 \cdot \underline{r}_2$$

$$= \tfrac{1}{2}(\underline{H}_0 - \underline{H}_{{}^1c}) \cdot \tfrac{1}{2}(\underline{H}_0 - \underline{H}_{{}^2c})$$

$$= \frac{1}{4}(\underline{H}_0 - \underline{H}_{{}^1c} - \underline{H}_{{}^2c} + \underline{H}_{{}^3c}) \;, \quad {}^3c = {}^1c \oplus {}^2c, \; \underline{H}_i \cdot \underline{H}_j = \underline{H}_{i \oplus j}$$

So, $$\underline{R}_{12} = \frac{1}{2^{2s}} \underline{\underline{H}}\, \underline{r}_{12}$$

$$= \frac{1}{2^{2s}} \underline{\underline{H}} \cdot \frac{1}{4}(\underline{H}_0 - \underline{H}_{1c} - \underline{H}_{{}^2c} + \underline{H}_{{}^3c})$$

$$= 2^{-(2s+2)} \Big[(\overset{0}{2^{2s}} \; 0 \ldots\ldots \overset{N-1}{0})^T - \\ (\overset{0}{0} \ldots \overset{{}^1c}{2^{2s}} \; 0 \ldots \overset{N-1}{0})^T - \\ (\overset{0}{0} \ldots \overset{{}^2c}{2^{2s}} \; 0 \ldots \overset{N-1}{0})^T + \\ (\overset{0}{0} \ldots \overset{{}^3c}{2^{2s}} \; 0 \ldots \overset{N-1}{0})^T \Big]$$

(b) $\underline{R}_3$:

$$r_3(x) = \bigoplus_{m=1}^{n} c_m x_m , \quad c = (c_n \ldots . c_1)$$

$$\text{So, } \underline{R}_3 = \tfrac{1}{2}\,(\overset{0}{1}\ 0 \ldots . \overset{c}{-1}\ 0 \ldots . \overset{N-1}{0}\ )^T \tag{4.23}$$

$$\text{Now, } b_{r_{12}r_3}(0) = 2^{2s} \sum_{t=0}^{N-1} (\underline{R}_{12} \cdot \underline{R}_3)_t \tag{4.24}$$

$$\underline{R}_{12}\underline{R}_3 = \tfrac{1}{4} \left[\begin{array}{c} 1 \\ 0 \\ \vdots \\ -1 \\ 0 \\ \vdots \\ -1 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{array}\right] \begin{array}{l} \leftarrow 0 \\ \\ \\ \leftarrow {}^1c \\ \\ \\ \leftarrow {}^2c \\ \\ \\ \leftarrow {}^3c \\ \\ \\ \\ \end{array} \times \tfrac{1}{2} \left[\begin{array}{c} 1 \\ 0 \\ \vdots \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{array}\right] \begin{array}{l} \leftarrow 0 \\ \\ \\ \\ \leftarrow c \\ \\ \\ \\ \end{array} \quad \text{(From (4.22) and (4.23))}$$

${}^1c$, ${}^2c$ and ${}^3c$ are fixed once f(x) and g(x) are known. As the dyadic shift, t, varies from 0 through N-1, it generates the set of all possible LBFs $\bigoplus_m c_m x_m$. So c goes through 0 to N-1. From the nature of the product, $\underline{R}_{12} \cdot \underline{R}_3$, we see four distinct possibilities for t; t is such that:

(a) $c={}^1c$

(b) $c={}^2c$

(c) $c={}^3c$

(d) $c \neq {}^1c$, ${}^2c$ or ${}^3c$.

<u>(a) and (b)</u>: $c = {}^1c \implies t = {}^2c,$ (from 4.15)

$c = {}^2c \implies t = {}^1c.$ (from 4.16)

For both of these,

$$\underline{R}_{12}\cdot\underline{R}_3 = \frac{1}{8}\begin{array}{cccccc} 0 & 1 & & c={}^1c \text{ or } {}^2c & & N-1 \\ (\,1 & 0 & \ldots & 1 & 0\ldots\ldots & 0\,)^T \end{array}$$

So, from (4.24),

$$b_{r_{12}r_3}(0) = 2^{2s-3}(1+1) = 2^{2s-2}$$

So, from (4.21),

$$\sum_x r_{12}(x)r_3(x) = 2^{2s-2} \qquad (4.25)$$

Substituting (4.19), (4.20) and (4.25) into (4.18), we get

$$\begin{aligned}\sum_{x=0}^{N-1} r(x,t) &= 2^{2s-2} + 2^{2s-1} - 2.2^{2s-2}\\ &= 2^{2s-2}\end{aligned}$$

So, number of ones of $r(x,t) = 2^{2s-2}$

number of zeros of $r(x,t) = 2^{2s} - 2^{2s-2} = 3.2^{2s-2}$

Thus, the difference$= 3.2^{2s-2} - 2^{2s-2} = 2^{2s-1}$.

Hence, $b_{fg}(t) = 2^{2s-1}$, for $t = {}^1c, {}^2c$ (4.26)

<u>(c)</u>: $c = {}^3c$

So, $t = {}^sc$ (from 4.17)

$$\underline{R}_{12}\cdot\underline{R}_3 = \frac{1}{8}\begin{array}{ccccc} 0 & 1 & & c={}^3c & & N-1 \\ 1 & 0 & \ldots. & -1 & 0\ldots. & 0\,)^T \end{array}$$

So, $b_{r_{12}r_3}(0) = 2^{2s-3}(1-1) = 0$

or $$\sum_x r_{12}(x)\, r_3(x) = 0 \qquad (4.27)$$

Substituting (4.19), (4.20) and (4.27) into (4.18), we get,

$$\sum_{x=0}^{N-1} r(x,t) = 2^{2s-2} + 2^{2s-1} - 0 = 3.2^{2s-2}$$

So, $b_{fg}(g) = 2^{2s} - 2.3.2^{2s-2}$

$= -2^{2s-1}$,

So, $b_{fg}(t) = -2^{2s-1}$, $t = {}^3c = {}^1c \oplus {}^2c$ (4.28)

(d): c is none of ${}^1c$, ${}^2c$ or ${}^3c$.

This implies that t is none of ${}^1c$, ${}^2c$ or ${}^3c$.

So, $\underline{R}_{12}.\underline{R}_3 = \frac{1}{8}(1\ 0.\ldots\ldots 0)^T$

or, $b_{r_{12}r_3}(0) = \sum_x r_{12}(x) r_3(x)$

$= 2^{2s-3}$

So, $\sum_{x=0}^{N-1} r(x,t) = 2^{2s-2} + 2^{2s-1} - 2.2^{2s-3}$

$= 2^{2s-1}$

Thus, $b_{fg}(t) = 0$

Hence, $b_{fg}(t) = 0$, $t \neq {}^1c$, ${}^2c$ or ${}^3c$ (4.29)

and if t gives rise to case B.

Some of the t's not equal to ${}^1c$, ${}^2c$ or ${}^3c$ will give rise to case C.

Case C: $r(x,t) = f(x) \oplus g(x) \oplus \sum_{m=1}^{n} c_m x_m \oplus 1$

$$= (x_i \oplus x_q)(x_j \oplus x_k) \oplus \sum_{m} c_m x_m \oplus 1$$

$$= r_{12}(x) \oplus r_3(x) \oplus 1 \text{ , } r_{12}(x) \text{ and } r_3(x) \text{ as before}$$

It is to be noted that this form cannot occur for $t = {}^1c$, ${}^2c$ or ${}^3c$ i.e. for this case c cannot be either one of ${}^1c$, ${}^2c$ or ${}^3c$.

As $g(x)$ has quadratic terms $x_i x_k$ and $x_j x_q$, for this case; if $c = {}^1c$, then $x_i x_q$ has to be a term of $g(x)$ which it is not; and if $c = {}^2c$, then $x_j x_k$ has to be a term of $g(x)$ which it is not; if $c = {}^3c$,

$$g(x) = g(x_n \ldots \bar{x}_i \ldots \bar{x}_q \ldots \bar{x}_j \ldots \bar{x}_j \ldots \bar{x}_k \ldots x_1)$$

$$= g(x) \oplus x_i \oplus x_q \oplus x_j \oplus x_k$$

which is not of the form of case C. So, for this case, the only alternative is of case B(d) i.e., $t \neq {}^1c$, ${}^2c$ or ${}^3c$.

For this as in case B(d),

$$b_{fg}(t) = 0 \tag{4.30}$$

Hence, from (4.14), (4.26), (4.28), (4.29) and (4.30) we get:

Lemma 4.8:

Let f(x) and g(x) be two N-point ($N=2^{2s}=2^{n}$) p-NRQFs related through a transposition (1)(2)...(jk)...(n). Let f(x) contain $x_i x_j \oplus x_k x_q$ and g(x), $x_i x_k \oplus x_j x_q$.

$$\text{Let } {}^{1}c = (\overset{n}{0}\ldots\overset{i}{1}\ 0\ldots\overset{q}{1}\ 0\ldots\overset{1}{0}),$$

$$ {}^{2}c = (\overset{n}{0}\ldots\overset{j}{1}\ 0\ldots\overset{k}{1}\ 0\ldots\overset{1}{0}) \text{ and}$$

${}^{3}c = {}^{1}C \oplus {}^{2}C$, then,

$$b_{fg}(t) = \begin{cases} 2^{2s-1} & , \ t=0,\ {}^{1}c,\ {}^{2}c \\ -2^{2s-1} & , \ t={}^{3}c \\ 0 & , \ \text{otherwise} \end{cases}$$

Lemma 4.7 and 4.8 jointly lead to another interesting result.

Corollary 4.1:

Cross-correlation between g(x) and ath dyadic shift of f(x), d(x), is

$$b_{dg}(t) = \begin{cases} 2^{2s-1} & , \ t=a,\ {}^{1}c\oplus a,\ {}^{2}c\oplus a \\ -2^{2s-1} & , \ t=a\oplus {}^{3}c \\ 0 & , \ \text{otherwise} \end{cases}$$

Hence, it follows that:

(i) number of non- zero values of $b_{fg}(t)$ is four;

(ii) three of these are 2^{2s-1} and the fourth is -2^{2s-1}.

We illustrate this with an example.

Example 4. 9: Let $f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$

and $g(x) = x_1x_2 \oplus x_3x_5 \oplus x_4x_6 \oplus x_7x_8$

be two p-NRQFs with $n = 2s = 8$, $N = 2^8 = 256$. The permutation cycle structure is

$$(1)(2)(3)(4\ 5)(6)(7)(8), \quad (j = 4,\ k = 5)$$

$f(x)$ contains $x_3x_4 \oplus x_5x_6$ $(i = 3,\ q = 6)$

$g(x)$ contains $x_3x_5 \oplus x_4x_6$.

So, ${}^1c = (00100100) = 36$

${}^2c = (00011000) = 24$

${}^3c = (00111100) = 60$

Hence,

$$b_{fg}(t) = \begin{cases} 128 , & t = 0,\ 24,\ 36 \\ -128 , & t = 60 \\ 0 , & \text{otherwise} . \end{cases}$$

Having found the cross-correlation for transposition-related p-NRQFs, we will generalise these for arbitrary p-NRQFs.

4.4.2 Cross-Correlation Between Arbitrary p-NRQfs

It is known that any arbitrary permutation cycle-structure relating two functions f(x) and g(x) can be obtained through a series of transposition-related intermediate functions. The cross-correlations between each of these pairs can be found out using the results of the previous section. Some relation connecting these pairwise correlations is in order. This important relation is derived below:

Lemma 49: Let f(x), g(x) and r(x) be three NRQFs of $n = 2s$ variables. Then,

$$b_{fg}(t) = \frac{1}{2^n} \sum_{k=0}^{2^n-1} b_{fr}(k)\ b_{rg}\ (k \oplus t).$$

In words, the cross-correlation between f and g, $\underline{b}_{fg}$ is 1/N times the cross-correlation between the correlation functions $\underline{b}_{fr}$ and $\underline{b}_{rg}$.

PROOF: $$\text{R.H.S.} = \frac{1}{N} \sum_{k=0}^{N-1} \underline{b}_{fr}(k)\ b_{rg}\ (k \oplus t).$$

In vector notation,

$$\text{R.H.S.} = \frac{1}{N} \cdot \frac{1}{N} \underline{\underline{H}} (\underline{B}_{fr} \cdot \underline{B}_{rg}),$$

where $\underline{B}_{fr} = \underline{\underline{H}}\ \underline{b}_{fr}$ and

$\underline{B}_{rg} = \underline{\underline{H}}\ \underline{b}_{rg}$.

Now, $\underline{B}_{fr} = (\underline{F} \cdot \underline{R})$ and

$\underline{B}_{rg} = (\underline{R} \cdot \underline{G})$, where

$\underline{F} = \underline{\underline{H}}\ {}^{c}\underline{f}$, $\underline{R} = \underline{\underline{H}}\ {}^{c}\underline{r}$ and $\underline{G} = \underline{\underline{H}}\ {}^{c}\underline{g}$

('c' ==> functions take the values $\{+1, -1\}$).

So, R.H.S. $= \frac{1}{N^2}\,\underline{\underline{H}}\,(\underline{F}.\underline{R}.\underline{R}.\underline{G})$

Now, $\underline{R} = (2^s \pm 2s\ldots\ldots \pm 2^s)^T$

Thus, $\underline{R}\,.\,\underline{R} = 2^{2s}\,(1\ 1\ldots\ldots\ 1)^T$

So, RHS $= \frac{1}{N^2}\,.\,N.\ \underline{\underline{H}}\,(\underline{F}\,.\,\underline{G})$

$= \frac{1}{N}\ \underline{\underline{H}}\,(\underline{F}\,.\,\underline{G})$

$= \underline{b}_{fg}$ Q.E.D.

If two p-NRQFs f(x) and g(x) are related through a series of transposition - related p-NRQFs as:

$$f(x),\ f_1(x),\ f_2(x),\ldots,\ f_m(x),\ g(x);$$

$\underline{f}, f_1$; f_1, f_2 ; ......$f_m g$ are the transposition - related pairs, then $\underline{b}_{ff_1}, \underline{b}_{f_1f_2}, \ldots \underline{b}_{f_m g}$ are known by the results of the previous section. Further, by using Lemma 4.8 repeatedly with the pairs $\underline{b}_{ff_1}, \underline{b}_{f_1f_2}$; $\underline{b}_{f_1f_2}, \underline{b}_{f_2f_3}$; .... $\underline{b}_{f_{m-1}f_m}$, $\underline{b}_{f_m g}$; $\underline{b}_{fg}$ can be found out.

In general, if two n variable functions f(x) and g(x) are related through an L-length permutation cycle

$$(i_1 i_2 \ldots i_L),$$

they can in turn be expressed as relations amongst (L-1) transpositions:

$(i_1 \quad i_L)$

$(i_1 \quad i_2)$

$(i_2 \quad i_3) \qquad ,i_1,i_2 \ldots i_L \in \{1, 2, \ldots, n\}$

$(i_{L-2} \; i_{L-1})$

<u>Example 4.20</u>:

$$\text{Let } f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \quad \text{and}$$

$$g(x) = x_1x_7 \oplus x_2x_4 \oplus x_3x_6 \oplus x_5x_8$$

The cycle structure is (1)(2357)(4)(6)(8). This can be obtained through the following series of transpositions:

$(1)(27)(3)(4)(5)(6)(8) \quad , (f \leftrightarrow f_1)$

$(1)(23)(4)(5)(6)(7)(8) \quad , (f_1 \leftrightarrow f_2)$

$(1)(2)(3\ 5)(4)(6)(7)(8) \quad , (f_2 \leftrightarrow g)$

The resulting series of functions is:

$$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$$

$$f_1(x) = x_1x_7 \oplus x_3x_4 \oplus x_5x_6 \oplus x_2x_8$$

$$f_2(x) = x_1x_7 \oplus x_2x_4 \oplus x_5x_6 \oplus x_3x_8$$

$$g(x) = x_1x_7 \oplus x_2x_4 \oplus x_3x_6 \oplus x_5x_8.$$

Firstly, $\underline{b}_{ff_1}$, $\underline{b}_{f_1f_2}$ and $\underline{b}_{f_2g}$ are found out.

$\underline{b}_{ff_1}$:

$r_1(x) = x_1 \oplus x_8 ; \qquad r_2(x) = x_2 \oplus x_7$

So, ${}^1c=(10000001)=129$; ${}^2c=(01000010)=66$

$${}^3c={}^1c \oplus {}^2c=(11000011) = 195$$

$$b_{ff_1}(t) = \begin{cases} 128 & , t=0,\ 66,\ 129 \\ -128 & , t=195 \\ 0 & , \text{otherwise} \end{cases}$$

$\underline{b}_{f_1f_2}$:

$$r_1(x) = x_2 \oplus x_3 \quad , \quad r_2(x) = x_4 \oplus x_8$$

So, ${}^1c=(00000110) = 6$, ${}^2c=(10001000) = 136$

$${}^3c=(10001110) = 142$$

So, $$b_{f_1f_2}(t) = \begin{cases} 128 & , t=0,\ 6,\ 136 \\ -128 & , t=142 \\ 0 & , \text{otherwise} \end{cases}$$

$\underline{b}_{f_2g}$:

$$r_1(x) = x_3 \oplus x_5 \quad , \quad r_2(x) = x_6 \oplus x_8$$

So, ${}^1c=(00010100) = 20$, ${}^2c=(10100000) = 160$

$${}^3c=(10110100) = 180$$

So, $$b_{f_2g}(t) = \begin{cases} 128 & , t=0,\ 20,\ 160 \\ -128 & , t=180 \\ 0 & , \text{otherwise} \end{cases}$$

An important point to note here is that for each transposition-related pair, $(f_i(x), f_j(x))$, $\{0, {}^1c, {}^2c, {}^3c\}$ i.e., the set of dyadic shifts for which $\underline{b}_{f_if_j}$ is non-zero, form an Abelian group with the group operation being $\oplus$. This is evident from Lemma 4.7. Also, every distinct transposition results in distinct ${}^1c$, ${}^2c$

and ^3c vis-a-vis another. As seen above, no two shifts except 0 for which $\underline{b}_{ff_1}$, $\underline{b}_{f_1f_2}$ and $\underline{b}_{f_2g}$ are non-zero, are same.

Now, $$b_{ff_2}(t) = \frac{1}{N} \sum_{x=0}^{N-1} b_{ff_1}(x)\; b_{f_1f_2}(x \oplus t)$$

This implies that $\underline{b}_{ff_2}$ is non-zero for all those t's for which,

$$^1x \oplus t = {}^2x,$$

where, ^1x and ^2x are the dyadic shifts for which $\underline{b}_{ff_1}$ and $\underline{b}_{f_1f_2}$ are non-zero, respectively.

So, $t = {}^1x \oplus {}^2x$, for all ^1x and ^2x,

and each $$b_{ff_2}(t) = \pm \frac{1}{2^{2s}} (2^{2s-1} . 2^{2s-1})$$
$$= \pm\, 2^{2s-2},$$

'+' if b_{ff_1} (^1x) and $b_{f_1f_2}$ (^2x) both are of the same sign and '-' if they are of opposite signs. This follows from the two properties mentioned above.

Using $\underline{b}_{ff_1}$ and $\underline{b}_{f_1f_2}$, non-zero $\underline{b}_{ff_2}(t)$'s are tabulated in Table 4.7.

For all other t's, $b_{ff_2}(t) = 0$.

So, $\underline{b}_{ff_2}$ has 4 times (16) the number of non-zero values of its component arrays $\underline{b}_{ff_1}$, $\underline{b}_{f_1f_2}$ but the magnitude is halfed to 2^{2s-2} obviously. These non-zero-$\underline{b}_{ff_2}$ dyadic shifts, t, also form a group because they constitute the set of all possible $\oplus$ sums of the elements of similar groups of each of the arrays $\underline{b}_{ff_1}$ and $\underline{b}_{f_1f_2}$.

Table 4.7

Figures in parenthesis are $b_{ff_2}(t)$

$t = {}^1x \oplus {}^2x$

${}^1x \backslash {}^2x$	0	6	136	142
0	0 (64)	6 (64)	136 (64)	142 (-64)
66	66 (64)	68 (64)	192 (64)	204 (-64)
129	129 (64)	135 (64)	9 (64)	15 (-64)
195	195 (-64)	197 (-64)	75 (-64)	141 (64)

No. of +ve values = 10 ; No. of -ve values = 6

= 3.3+1 ; = 3.1 + 3.1 = 6

Similarly,

$$b_{fg}(t) = \frac{1}{2^{2s}} \sum_{x=0}^{N-1} b_{ff_2}(x)\ b_{f_2g}(x \oplus t).$$

Again, using similar arguments as for $\underline{b}_{ff_2}$, we compute the dyadic shifts, t, for which $\underline{b}_{fg}$ is non-zero, in Table 4.8.

Again, the number of non-zero values has increased four-fold to 64 and their magnitude has decreased by half to 32.

Number of +ve values = 10 x 3 + 6 x 1 = 36

Number of -ve values = 10 x 1 + 3 x 6 = 28.

The t's again form a group.

Table 4.8

Figures in parenthesis are the correlations

$t = {}^{1}x \oplus {}^{2}x$

^{2}x ^{1}x	0		20		160		180	
0	0	(32)	20	(32)	160	(32)	180	(-32)
6	6	(32)	18	(32)	166	(32)	178	(-32)
136	136	(32)	156	(32)	40	(32)	60	(-32)
142	142	(-32)	154	(-32)	46	(-32)	58	(32)
66	66	(32)	86	(32)	226	(32)	246	(-32)
68	68	(32)	80	(32)	228	(32)	240	(-32)
192	192	(32)	222	(32)	106	(32)	126	(-32)
204	204	(-32)	216	(-32)	108	(-32)	120	(32)
129	129	(32)	149	(32)	33	(32)	53	(-32)
135	135	(32)	147	(32)	39	(32)	51	(-32)
9	9	(32)	29	(32)	169	(32)	189	(-32)
15	15	(-32)	27	(-32)	175	(-32)	187	(32)
195	195	(-32)	215	(-32)	99	(-32)	119	(32)
197	197	(-32)	209	(-32)	101	(-32)	113	(32)
75	75	(-32)	95	(-32)	235	(-32)	255	(32)
141	141	(32)	89	(32)	237	(32)	249	(-32)

These results are generalised below:

Lemma 4.10: If two $n = 2s$ variable NRQFs, $f(x)$ and $g(x)$, are related through t transpositions, then:

(a) Number of non-zero values of $\underline{b}_{fg} = (4)^{t} = 2^{2t}$,

(b) Magnitude of the values $= (\frac{1}{2})^{t-1}.2^{2s-1}$

$= 2^{2s-t}$

(c) Number of positive values = $2^{2t-1} + 2^{t-1}$

(d) Number of negative values = $2^{2t-1} - 2^{t-1}$, and

finally, (e) all the dyadic-shifts, resulting in non-zero $b_{fg}(a)$ form a group with $\oplus$ as the group operation.

An s-length permutation cycle is the longest possible between two NRQFs, f(x) and g(x), of $n = 2s$ variables. So, least cross-correlation magnitude achievable according to (b) is

$$2^{2s-(s-1)}, \; t=s-1 \text{ here.}$$

$$= 2^{s+1} = 2(N)^{\frac{1}{2}} \text{, where } N = 2^{2s} \text{ is the length of NRQFs.}$$

So, $\lim\limits_{N \to \infty} \dfrac{2(N)^{\frac{1}{2}}}{N} = \lim\limits_{N \to \infty} \dfrac{2}{(N)^{\frac{1}{2}}} = 0$.

Hence, asymptotically-ideal cross-correlation is achievable with NRQFs.

Representative examples for $\underline{b}_{fg}$ for $n = 8$ variables and various permutation cycle structures - viz. one 2-length cycle (one transposition), one 3-length cycle (two transpositions), two 2-length cycles (two transpositions) and one 4-length cycle (three transpositions) - are given in Tables 4.9, 4.10, 4.11 and 4.12.

This brings us to the end of dyadic correlation analysis of NRQFs. Cross-correlation between NRQFs related through arbitrary permutations has been found out. Enumeration of all possible L-length permutation cycles for an NRQF will complete the picture.

Table 4.9

Functions f and g related thru one 2-length permutation cycle

$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$ $g(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_7 \oplus x_6x_8$

Cycle Structure : (1)(2)(3)(4)(5)(67)(8)

$b_{fg}(k)$	k's
128	0 96 144
-128	240
0	otherwise

Table 4.10

Functions f and g related thru one 3-length permutation cycle

$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$ $g(x) = x_1x_7 \oplus x_2x_4 \oplus x_5x_6 \oplus x_3x_8$

Cycle Structure : (1)(237)(4)(5)(6)(8)

$b_{fg}(k)$	k's
64	0 6 9 66 68 77 129 135 136 202
-64	15 75 142 195 197 204
0	otherwise

Table 4.11

Functions f and g related thru two 2-length permutation cycles

$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$ $g(x) = x_1x_5 \oplus x_3x_7 \oplus x_2x_6 \oplus x_4x_8$

Cycle structure : (1)(25)(3)(47)(6)(8)

$b_{fg}(k)$	k's
64	0 18 33 72 90 105 132 150 165 255
-64	51 123 183 204 222 237
0	otherwise

where each $L_i > 1$ and $\sum_{i=1}^{m} L_i \leqslant s$.

Example 4.21: For n = 8 variables, consider the p-NRQF

$$f(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$$

Number of p-NRQFs of 8 variables = N(8) = 105

" " single 2-length permutation cycles of f = $^4C_2 . 2^1 . (1)! = 12$

" " single 3-length permutation cycles of f = $^4C_3 . 2^2 . (2)! = 32$

" " single 4-length permutation cycles of f = $^4C_4 . 2^3 (3)! = 48$

" " two 2-length permutation cycles of f = $^4C_2 . (^2C_2 . 2^1 . (1)!)$

$= 6 \times 2 = 12$

This exhausts all possible p-NRQFs of 8 variables.

Some computed results on the periodic and aperiodic correlation parameters of p-NRQFs are presented now.

4.6 SOME RESULTS ON THE PERIODIC AND APERIODIC CORRELATION PARAMETERS OF p-NRQFs

Let $C_{uv}(t)$ and $p_{uv}(t)$ be the aperiodic and periodic cross-correlations between two p-NRQFs u and v of length $N = 2^n$.

$$p_{uv}(t) = C_{uv}(t) + C_{uv}(t-N), \quad 0 \leqslant t \leqslant N-1$$

This is also called even cross-correlation whereas odd cross-correlation, $\hat{p}_{uv}(t)$, is:

$$\hat{p}_{uv}(t) = C_{uv}(t) - C_{uv}(t-N) \,, \qquad 0 \leqslant t \leqslant N-1 \,.$$

$p_u(t)$ and $\hat{p}_u(t)$ are the even and odd autocorrelation functions. Certain correlation parameters of importance in SS-CDMA systems [Pursby and Roefs, 1979] are:

(1) Peak even cross-correlation, $M(u,v)$,

$$M(u,v) \triangleq \max\left\{ |p_{uv}(t)| : 0 \leqslant t \leqslant N-1 \right\};$$

(2) Peak odd cross-correlation, $\hat{M}(u,v)$,

$$\hat{M}(u,v) \triangleq \max\left\{ |\hat{p}_{uv}(t)| : 0 \leqslant t \leqslant N-1 \right\};$$

(3) Peak out-of-phase even auto-correlation, $M(u)$,

$$M(u) \triangleq \max\left\{ |p_u(t)| : 1 \leqslant t \leqslant N-1 \right\};$$

(4) Peak out-of-phase odd auto-correlation, $\hat{M}(u)$,

$$\hat{M}(u) \triangleq \max\left\{ |\hat{p}_u(t)| : 1 \leqslant t \leqslant N-1 \right\};$$

(5) $\hat{L}(u) = \| \{ t : |\hat{p}_u(t)| = \hat{M}(u) \,,\ 1 \leqslant t \leqslant N-1 \}$, where $\|A\|$ is cardinality of A. $\hat{L}(u)$ is the number of occurrences of $\hat{M}(u)$ in $\hat{p}_u(t)$;

(6) Sidelobe energy,

$$S(u) = \sum_{t=1}^{N-1} C_u^{\,2}(t)$$

The relevant parameters for p-NRQFs have been found in the following way:

(i) Auto-optimal (AO) phase of the p-NRQF is found out.

The phase j of a sequence $\underline{u}$ is an auto-optimal phase if $\hat{M}(T^j \underline{u}) = \hat{p}_{AO}(\underline{u})$ and if $\hat{L}(T^j\underline{u})$ is the minimum of $\hat{L}(T^i\underline{u})$ over all i for which $\hat{M}(T^i\underline{u}) = \hat{p}_{AO}(\underline{u})$.

In other words, $\hat{M}(u)$ is found out for each of the N-phases of the NRQF $\underline{u}$ and number of times it occurs in each phase is also computed. Then, minimum of $\hat{M}(u)$ over all phases is computed. Say, $\hat{M}(T^j\underline{u})$ is this minimum. But there can be many j's with this $\hat{M}(\underline{u})$. So, those j's are chosen for which number of occurrences of $\hat{M}(\underline{u})$, $\hat{L}(\underline{u})$, are a minima. Even then there can be more than one such phases. These are the auto-optimal phases.

(ii) Amongst the auto-optimal phases, those are chosen for which $\underline{u}$ has the minimum sidelobe energy, S(u). Now, only one or a few phases are left. This/these is/are the AO/LSE p-NRQF.

(iii) (i) and (ii) are repeated for each p-NRQF of n variables.

(iv) Peak odd, and even cross-correlations, $\hat{M}(u,v)$ and $M(u,v)$, are computed for each pair of AO/LSE p-NRQFs of n variables.

(v) Peak even out-of-phase auto-correlation of each p-NRQF is computed.

It is to be noted that,

$$M(u,v) = M(v,u) \text{ and } \hat{M}(u,v) = \hat{M}(v,u)$$

Correlation parameters for all p-NRQFs of 4 and 6 variables and for some of 8 variables have been computed following the above procedure. Results are reported in Tables 4.13 and 4.14.

Table 4.13

AO/LSE Phases of p-NRQFs of 4,6- and 8 Variables

n	N	p-NRQF(u)	AO/LSE Phase(s)	$\hat{M}(u)$	$\hat{L}(u)$	$\dot{S}(u)$
4	16	12 34	6	2	8	24
		13 24	3	2	8	24
		14 23	4,7,12,15	6	2	40
6	64	12 34 56	26	10	4	752
		12 35 46	12	14	4	928
		12 36 45	43	20	4	1480
		13 24 56	20	16	2	1088
		13 25 46	21,53	14	4	1272
		13 26 45	21	12	10	1096
		14 23 56	21	12	4	992
		14 25 36	41	12	4	1112
		14 26 35	11	12	2	1152
		15 34 26	12	14	2	992
		15 23 46	54	14	2	1088
		15 36 24	11	12	2	1000
		16 34 25	9,41	12	2	840
		16 32 45	20,52	10	6	816
		16 35 24	9,41	12	2	1064
8	256	12 34 56 78	102	50	2	20720
		12 34 57 68	47	56	4	21824
		17 24 56 38	167	48	6	28688
		17 24 36 58	215	52	2	29456
		15 37 26 48	80	58	2	31744

Table 4.14

Peak Correlation Parameters for AO/LSE p-NRQFs

(a) $n = 4$, $N = 16$

p-NRQF	12 34	13 24	14 23
12 34	4	8	8
13 24	10	4	8
14 23	10	8	4

(b) $n = 6$, $N = 64$

p-NRQF	12 34 56	12 35 46	12 36 45	13 24 56	13 25 46	13 26 45	14 22 56	14 25 36	14 26 35	15 34 26	15 23 46	15 36 24	16 34 25	16 32 45	16 35 24
12 34 56	16	32	32	32	16	16	32	16	16	32	20	20	32	16	16
12 35 46	36	16	32	16	32	16	16	24	32	16	32	24	16	20	32
12 36 45	26	30	16	16	16	16	32	16	16	16	32	20	20	32	20
13 24 56	24	20	28	20	32	32	32	20	16	20	16	32	16	16	32
13 25 46	18	26	14	30	16	32	16	32	16	24	32	16	32	20	20
13 26 45	18	16	18	30	32	16	16	16	32	32	16	16	16	32	16
14 23 56	30	18	32	30	22	22	16	32	32	20	32	16	16	32	16
14 25 36	18	20	16	18	20	20	20	20	32	20	20	32	32	16	24
14 26 35	20	30	14	18	20	20	24	20	16	32	16	16	16	20	32
15 34 26	20	16	14	18	24	30	30	18	34	16	32	32	32	20	16
15 23 46	24	26	24	20	18	22	26	20	24	24	16	32	16	32	16
15 36 24	20	24	20	30	22	16	18	22	16	34	18	16	16	16	32
16 34 25	24	20	18	20	18	22	20	22	20	26	18	18	16	32	32
16 32 45	16	20	22	22	20	30	30	20	20	20	24	18	26	16	32
16 35 24	20	30	20	22	22	22	18	22	36	20	20	28	32	22	20

...contd.

(c) $n = 8$, $N = 256$

p-NRQFs	1 2 3 4 5 6 7 8	1 2 3 4 5 7 6 8	1 2 2 4 5 6 3 8	1 2 2 4 3 6 5 8	1 2 3 7 2 6 4 8
12 34 56 78	64	128	68	40	64
12 34 57 68	146	64	40	48	40
17 24 56 38	56	42	64	128	48
17 24 36 58	52	48	80	64	44
15 37 26 48	56	46	48	44	84

In the tables for peak correlation parameters, entries above the diagonal are for $M(u,v)$, $\hat{M}(u,v)$ is given below the diagonal and $M(u)$ is along it.

From the data available, it is conjectured that minimum odd cross-correlation which can be achieved with N-length p-NRQFs is $\frac{N}{4}$. $\frac{C_{\hat{p}\,max}}{N} = \frac{1}{4}$ tends to remain constant as N increases unlike the case of m-sequences, where this ratio asymptotically goes to zero amongst certain sets of sequences. Hence, periodic and aperiodic correlation performance is much worse vis-a-vis m-sequences. More data needs to be analysed to draw any further conclusions..

It is to be noted that NRQFs are not the only binary Boolean functions with uniform-magnitude sequency-spectrum.

Example 4.22: The repetitive quadratic form

$$f_1(x) = x_1x_2 \oplus x_3x_4 \oplus x_2x_3$$ and another degree three function,

$$f_2(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$$

are two non-NRQFs with uniform - magnitude sequency spectrum.

The general class of these functions, called bent functions, is discussed in the next chapter.

CHAPTER 5

BENT FUNCTIONS

This chapter, the results of which were already available, is included to complete the notion of NRQFs introduced in the previous chapter in which the work done had been completely independent of this.

The notion of NRQFs is generalised to that of bent functions in this chapter. Sections 5.1 and 5.2 deal with their definition and some of the properties. Section 5.3 presents the problems encountered in the enumeration of bent functions of a given number of variables. Section 5.4 goes on to the subclass of quadratic bent functions, their graphical representation and their exhaustive enumeration. Auto-correlation of bent functions is derived in Section 5.5.

5.1 DEFINITION [MacWilliams and Sloane, 1977; Rothaus, 1976]

Let $f(x)$ be a binary Boolean function of $n = 2s$ variables.

Let ${}^{c}f(x) = 1-2f(x)$ i.e., $f(x)$ in the $\{1,-1\}$ form;

and $\underline{F} = \underline{\underline{H}}\ {}^{c}f$ be the u-WHT of ${}^{c}\underline{f}$.

Then $f(x)$ is called a bent function iff each WHT coefficient, F_i, is $\pm 2^{n/2}$ $(\pm 2^{s})$.

The already encountered NRQFs satisfy this condition. An example of a non-NRQF bent function is:

Example 5.1: Let $f(x) = x_1x_2 \oplus x_2x_3 \oplus x_3x_4$ be a $\{0,1\}$ valued function of 4 variables. $\underline{f}$, $^c\underline{f}$ and $\underline{F}$ are as in Table 5.1.

Table 5.1

WHT of $f(x) = x_1x_1 \oplus x_2x_3 \oplus x_3x_4$

x	$(x_4x_3x_2x_1)$	f	$^c\underline{f}$	$\underline{F}$
0	0 0 0 0	0	1	4
1	0 0 0 1	0	1	4
2	0 0 1 0	0	1	4
3	0 0 1 1	1	-1	-4
4	0 1 0 0	0	1	4
5	0 1 0 1	0	1	4
6	0 1 1 0	1	-1	4
7	0 1 1 1	0	1	-4
8	1 0 0 0	0	1	4
9	1 0 0 1	0	1	-4
10	1 0 1 0	0	1	4
11	1 0 1 1	1	-1	4
12	1 1 0 0	1	-1	-4
13	1 1 0 1	1	-1	4
14	1 1 1 0	0	1	-4
15	1 1 1 1	1	-1	-4

It is easy to see that this bent function, called a quadratic form, is an Affine Transformation of the p-NRQF,

$$g(x) = x_1x_2 \oplus x_3x_4$$

(Two n variable binary functions f(x) and g(x) are said to be related through an affine transformation iff

$f(x) = g\ (x\ \underline{\underline{A}} \oplus \underline{B})$, where $\underline{\underline{A}}$ is an n x n invertible binary matrix and $\underline{B}$ is a 1 x n binary vector).

In the above case,

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \underline{B}\ (0\ 0\ 0\ 0)$$

$$\begin{aligned} g(x\ \underline{\underline{A}} \oplus \underline{B}) &= (x_1 \oplus x_3)\ x_2 \oplus x_3x_4 \\ &= x_1x_2 \ominus x_2x_3 \ominus x_3x_4 \\ &= f(x). \end{aligned}$$

5.2 PROPERTIES OF BENT FUNCTIONS

Let f(x) be a bent function of n variables.

(1) n is even i.e., bent functions exist only for an even number of variables, $n = 2s$ and if $n > 2$, then deg $f \leq \frac{1}{2}$ n.

(2) 2^{-s} times the u-WHT of a bent function of $n = 2s$ variables is also bent.

$\underline{F} = \underline{\underline{H}}\ {}^{c}\underline{f}$ is u-WHT of $\underline{f}$.

$F_i = \pm\ 2^s$, $i = 0, 1, \ldots, 2^n - 1$.

So, $2^{-s}.F_i = \pm\ 1 = (-1)^{f_d(i)}$, where $f_d(i)$ is another Boolean function.

So, $2^{-s}\ \underline{F}$ defines another function $\underline{f}_d$.

Let ${}^{c}\underline{f}_d = 1 - 2\,\underline{f}_d$

Now, if $\underline{F}^d = \underline{\underline{H}}\;{}^{c}\underline{f}_d$,

then, $F^d(i) = \underline{+}2^s$.

Hence, $\underline{f}_d$ is also a bent function.

f(x) has a natural partner in $f_d(x)$ through its WHT. It is possible for certain bent functions that $\underline{f}$ and $\underline{f}_d$ are same.

i.e., $$\underline{\underline{H}}\;{}^{c}\underline{f} = 2^s\;{}^{c}\underline{f} \tag{5.1}$$

It is obvious that such functions are the eigenvectors of the Hadamard matrix $\underline{\underline{H}}$.

<u>Conjecture:</u> All the p-NRQFs of n variables are eigenvectors of the N x N $(N = 2^n)$ Hadamard matrix $\underline{\underline{H}}$.

This has been verified for 2, 4, 6 and 8 variable p-NRQFs.

<u>Example 5.2:</u> $\underline{f}$, $\underline{F}$ and $\underline{f}_d$ for the three p-NRQFs of 4 variables:

${}^{1}f(x) = x_1x_2 \oplus x_3x_4$

${}^{2}f(x) = x_1x_3 \oplus x_2x_4$ and

${}^{3}f(x) = x_1x_4 \oplus x_2x_3$ are shown in Table 5.2.

(3) $\underline{F} = \underline{\underline{H}}\;{}^{c}\underline{f}$

$F_o = \underline{+}\ 2^s$.

Let Z_o = Number of zeros of $\underline{f}$

Z_1 = Number of ones of $\underline{f}$.

Table 5.2

$\underline{f}$, $\underline{F}$ and $\underline{f}_d$ for ${}^1f(x)$, ${}^2f(x)$ and ${}^3f(x)$:

$$ {}^1f(x) = x_1x_2 \oplus x_3x_4 $$
$$ {}^2f(x) = x_1x_3 \oplus x_2x_4 $$
$$ {}^3f(x) = x_1x_4 \oplus x_2x_3 $$

x	$(x_4x_3x_2x_1)$	${}^1\underline{f}$	${}^1\underline{F}$	${}^1\underline{f}_d$	$\underline{f}$	${}^2\underline{F}$	${}^2\underline{f}_d$	${}^3\underline{f}$	${}^3\underline{F}$	${}^3\underline{f}_d$
0	0 0 0 0	0	4	0	0	4	0	0	4	0
1	0 0 0 1	0	4	0	0	4	0	0	4	0
2	0 0 1 0	0	4	0	0	4	0	0	4	0
3	0 0 1 1	1	-4	1	0	4	0	0	4	0
4	0 1 0 0	0	4	0	0	4	0	0	4	0
5	0 1 0 1	0	4	0	1	-4	1	0	4	0
6	0 1 1 0	0	4	0	0	4	0	1	-4	1
7	0 1 1 1	1	-4	1	1	-4	1	1	-4	1
8	1 0 0 0	0	4	0	0	4	0	0	4	0
9	1 0 0 1	0	4	0	0	4	0	1	-4	1
10	1 0 1 0	0	4	0	1	-4	1	0	4	0
11	1 0 1 1	1	-4	1	1	-4	1	1	-4	1
12	1 1 0 0	1	-4	1	0	4	0	0	4	0
13	1 1 0 1	1	-4	1	1	-4	1	1	-4	1
14	1 1 1 0	1	-4	1	1	-4	1	1	-4	1
15	1 1 1 1	0	4	0	0	4	0	0	4	0

So, $Z_o - Z_1 = \pm\, 2^s$ and

$Z_o + Z_1 = 2^{2s}$.

Thus, $Z_o = \begin{cases} 2^{2s-1} + 2^{s-1} \\ \\ 2^{2s-1} - 2^{s-1} \end{cases}$ $\qquad Z_1 = \begin{cases} 2^{2s-1} - 2^{s-1} \\ \\ 2^{2s-1} + 2^{s-1} \end{cases}$

Hence, a necessary condition for f(x) to be a bent function is that its number of ones and zeros should be one of the above sets of values.

(4) Any affine transformation of f(x) results in another bent function.

<u>PROOF:</u> $$F(m) = \sum_{i=0}^{2^n-1} (-1)^{\langle m,i\rangle} (-1)^{f(m)}$$

$$= \underline{+}2^s$$

Let $g(x) = f(x\,\underline{\underline{A}} \oplus \underline{B})$, be an affine transformation of f(x).

So, $$G(m) = \sum_{i=0}^{N-1} (-1)^{\langle m,i\rangle} (-1)^{f(i\,\underline{\underline{A}} \oplus \underline{B})} \quad , \; N = 2^n$$

Let $k = i\,\underline{\underline{A}} \oplus \underline{B}$

or $i = (k \oplus \underline{B})\,\underline{\underline{A}}^{-1}$

So, $$G(m) = \sum_{k=0}^{N-1} (-1)^{\langle m,\, (k\oplus\underline{B})\,\underline{\underline{A}}^{-1}\rangle} (-1)^{f(k)}$$

$$= \sum_{k} (-1)^{\langle m',k\rangle} \cdot (-1)^{\langle m,\, \underline{B}\underline{\underline{A}}^{-1}\rangle} \cdot (-1)^{f(k)},$$

where $m' = m(\underline{\underline{A}}^{-1})^T$

$$= (\underline{+}\,1) \cdot \sum_{k} (-1)^{\langle m',k\rangle} \cdot (-1)^{f(k)} \; ,$$

as $(-1)^{\langle m,\underline{B}\,\underline{\underline{A}}^{-1}\rangle} = (\underline{+}1)$.

$= (\underline{+}\,1).F(m')$, as m varies from 0 to N-1, m′ also takes all these values.

Thus, $G(m) = \pm 2^{s}$.

Hence, $g(x)$ is also a bent function. Q.E.D.

(5) Complement of a bent function is also bent.

Properties 4 and 5 can be used to find bent functions of a given number of variables.

5.3 NOTE ON THE ENUMERATION OF BENT FUNCTIONS

Unfortunately, there is no known elegant method of enumerating all bent functions of a given number of variables. Property 4 holds that affine transformations divide the set of bent functions into various equivalence classes. But, it does not give the representative function of each class whose affine transformations are the rest.

In general, to find this representative function, a brute force approach using the definition of bent functions can be adopted. 2^n-point binary functions with weights $(2^{2s-1}-2^{s-1})$ are selected and their u-WHTs found one-by-one. If a bent function is encountered, all its affine transformations are grouped together and deleted from the set. Complements of these functions are also bent.

Number of affine transformations for $n = 2s$ variables

$$= 2^{n} . \prod_{i=0}^{n-1} (2^{m}-2^{i}) \text{, and}$$

number of binary functions with weight $(2^{2s-1}-2^{s-1}) = \left(\begin{matrix} 2^{2s} \\ 2^{2s-1}-2^{s-1} \end{matrix} \right.$

Hence, this method becomes impractical as n increases because number of possible functions to be checked increases exponentially.

If generalised bent functions are defined as real valued 2^n-point($N = 2^n$, $n = 2s$) functions with uniform-magnitude sequency spectrum, then these can be exhaustively enumerated. If $\underline{f}$ is such a function,

$$\underline{\underline{H}}\ \underline{f} = (N)^{\frac{1}{2}}\ \underline{g}\ ,\ \text{where } \underline{g} \text{ is a} \left\{+1,-1\right\} - \text{valued function.}$$

$$\underline{f} = \frac{1}{(N)^{\frac{1}{2}}}\ \underline{\underline{H}}\ \underline{g} \qquad (5.2)$$

As $\underline{f}$ is real-valued, all possible 2^{2^n} $\left\{+1,\ -1\right\}$ valued 2^n-point functions $\underline{g}$ will result in distinct generalised bent functions $\underline{f}$ of n variables. This set will be complete.

<u>Example 5.3</u>: Consider the generalised bent functions of 2 variables. Number of functions $\underline{g}$ is 2^{2^2} i.e. 16. The 16 bent functions computed using (5.2) are:

$\underline{g}_o$	1	1	1	1	$\underline{f}_o$	2	0	0	0
$\underline{g}_1$	1	1	1	-1	$\underline{f}_1$	1	1	1	-1
$\underline{g}_2$	1	1	-1	1	$\underline{f}_2$	1	-1	1	1
$\underline{g}_3$	1	1	-1	-1	$\underline{f}_3$	0	0	2	0
$\underline{g}_4$	1	-1	1	1	$\underline{f}_4$	1	1	-1	1
$\underline{g}_5$	1	-1	1	-1	$\underline{f}_5$	0	2	0	0
$\underline{g}_6$	1	-1	-1	1	$\underline{f}_6$	0	0	0	2
$\underline{g}_7$	1	-1	-1	-1	$\underline{f}_7$	-1	1	1	1

$\underline{g}_8$	-1	1	1	1	$\underline{f}_8$	1	-1	-1	-1
$\underline{g}_9$	-1	1	1	-1	$\underline{f}_9$	0	0	0	-2
$\underline{g}_{10}$	-1	1	-1	1	$\underline{f}_{10}$	0	-2	0	0
$\underline{g}_{11}$	-1	1	-1	-1	$\underline{f}_{11}$	-1	-1	1	-1
$\underline{g}_{12}$	-1	-1	1	1	$\underline{f}_{12}$	0	0	-2	0
$\underline{g}_{13}$	-1	-1	1	-1	$\underline{f}_{13}$	-1	1	-1	-1
$\underline{g}_{14}$	-1	-1	-1	1	$\underline{f}_{14}$	-1	-1	-1	1
$\underline{g}_{15}$	-1	-1	-1	-1	$\underline{f}_{15}$	-2	0	0	0

Again, for these computations, only representative functions of each equivalence class need be computed and the rest are their affine transformations or complements. For instance, computation of $\underline{f}_0$, $\underline{f}_1$, $\underline{f}_3$, $\underline{f}_5$ and $\underline{f}_6$ is sufficient for finding out the rest.

Hence, in general, the enumeration of bent functions is still an open problem. However, a class of bent functions, called quadratic bent functions, is enumerable.

5.4 QUADRATIC BENT FUNCTIONS

Bent functions consisting of quadratic (degree 2) terms only are called quadratic bent functions (QBFs). It is possible to find the total number of QBFs of a given number of variables in general.

Any quadratic form (not necessarily bent), f(v), of n variables can be expressed in terms of an n x n upper triangular binary matrix $\underline{\underline{Q}}$. q_{ij} is one iff v_iv_j is a term of $f(v)$.

Example 5.4: Consider the QBF, $f(v)$, of 4 variables,

$$f(v) = v_1v_2 \oplus v_3v_4.$$

Alternatively, it is expressible as:

$$f(v) = \begin{bmatrix} v_1 v_2 v_3 v_4 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}$$

$$= \underline{v}\ \underline{\underline{Q}}\ \underline{v}^T,$$

where $$\underline{\underline{Q}}(v) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Similarly,

$$\underline{\underline{Q}} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$ represents

$$g(v) = \underline{v}\ \underline{\underline{Q}}\ \underline{v}^T$$

$$= v_1v_2 \oplus v_1v_4 \oplus v_2v_3 \oplus v_3v_4$$

$g(v)$ is not a QBF.

Further, a quadratic form, $f(v)$, can be characterised by a symmetric matrix,

$$\underline{\underline{S}} = \underline{\underline{Q}} \oplus \underline{\underline{Q}}^T$$

$\underline{\underline{S}}$ generates another form which is symmetric bilinear, called a symplectic form, the matrix $\underline{\underline{S}}$ being termed as symplectic matrix. This form, in general, for a given $\underline{\underline{S}}$ is :

$$S(u,v) = \underline{u}\ \underline{\underline{S}}\ \underline{v}^T \quad , \quad \begin{aligned} \underline{u} &= [u_1 \ldots u_n] \\ \underline{v} &= [v_1 \ldots v_n] \\ \underline{\underline{S}} &= (s_{ij})_{n \times n} . \end{aligned}$$

<u>Example 5.5</u>: Matrix $\underline{\underline{S}}$ for the QBF of previous example is:

$$\underline{\underline{S}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$S(u,v) = \begin{bmatrix} u_1 u_2 u_3 u_4 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}$$

$$= u_2 v_1 \oplus u_1 v_2 \oplus u_4 v_3 \oplus u_3 v_4$$

Evidently, each quadratic form has a unique $\underline{\underline{Q}}$ and $\underline{\underline{S}}$ representation and vice-versa. Whether a form is bent depends on the rank of $\underline{\underline{S}}$.

<u>Lemma 5.1:</u>

Let N(m,r) be the number of m x m symplectic matrices of rank r over GF(2). Then,

$$N(m,\ r = 2h+1) = 0 \text{ and}$$

$$N(m, r = 2h) = \frac{(2^m-1)(2^{m-1}-1)\ldots(2^{m-2h+1}-1)}{(2^{2h}-1)(2^{2h-2}-1)\ldots(2^2-1)} \cdot 2^{h(h-1)}$$

Lemma 5.2:

A quadratic form, $f(v)$, of m variables is a bent function iff its symplectic matrix $\underline{\underline{S}}$ has rank $r=m$ i.e. $2h=m$.

Example 5.6:

(i) Let $f(v) = v_1v_2 \oplus v_2v_3 \oplus v_3v_4 \oplus v_1v_3$ be a quadratic form of 4 variables:

$$\underline{\underline{S}} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Rank ($\underline{\underline{S}}$) = 4. So, $f(v)$ is a bent function.

(ii) Let $g(v) = v_1v_2 \oplus v_2v_3 \oplus v_1v_4 \oplus v_3v_4$

$$\underline{\underline{S}} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$g(v)$ is not a bent function because rank ($\underline{\underline{S}}$) = 2.

For small values of m (say $m \leqslant 6$), whether a quadratic form is a bent function can be found out by inspection from its $\underline{\underline{S}}$ matrix.

Lemmas 5.1 and 5.2 jointly give the total number of possible quadratic bent functions of a given number of variables. Number of quadratic bent functions of $m = 2s$ variables is the number of binary $m \times m$ symplectic matrices with rank $r = m$ which is:

$$N(m, r = m) = \frac{(2^m - 1)(2^{m-1} - 1)\ldots(2^1 - 1)}{(2^m - 1)(2^{m-2} - 1)\ldots(2^2 - 1)} \cdot 2^{s(s-1)}$$

$$= (2^{m-1} - 1)(2^{m-3} - 1)\ldots(2^1 - 1) \cdot 2^{s(s-1)}$$

For $m = 4$, $N = 28$

For $m = 6$, $N = 13888$

For $m = 8$, $N = 112881664$

These do not include the functions with complementation of variables.

<u>Lemma 5.3</u>:

Any quadratic bent function of m variables is an affine transformation of the principal form

$$f_p(v) = v_1 v_2 \oplus v_3 v_4 \oplus \ldots \oplus v_{m-1}\; v_m \oplus e, \quad e \in \{0, 1\}$$

e.g. bent functions of $m = 4$ variables are all quadratic forms. They can be divided into four different classes having two, three, four and six quadratic terms respectively, each being expressed as an affine transformation of the principal form.

(1) ${}^1f(v) = v_1 v_2 \oplus v_3 v_4$ (3 types)

(2) ${}^2f(v) = v_1 v_2 \oplus v_2 v_3 \oplus v_3 v_4$ (12 types)

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \underline{B} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad e = 0$$

$${}^2f(v) = {}^1f(\underline{\underline{A}}\, v \oplus \underline{B}).$$

(3) $^{3}f(v) = v_1v_2 \oplus v_2v_3 \oplus v_3v_4 \oplus v_1v_3$ (12 types)

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \underline{B} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} , \quad e = 1$$

$$^{3}f(v) = {}^{1}f\,(\underline{\underline{A}}\ \underline{v} \oplus \underline{B}\,)$$

(4) $^{4}f(v) = v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ (1 type)

$$\underline{\underline{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \underline{B} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} , \quad e = 1$$

$$^{4}f(v) = {}^{1}f\,(\underline{\underline{A}}\ \underline{v} \oplus \underline{B}) \text{ with } e = 1$$

The graphical representations of these 28 bent functions are given in Table 5.3.

5.5 AUTO-CORRELATION PROPERTY OF BENT FUNCTIONS

Theorem: A Boolean function f(v) of $m = 2s$ variables is a bent function iff its dyadic auto-correlation is of the form:

$$b_f(t) = \begin{cases} 2^{2s} & , \ t = 0 \\ 0 & , \ t = 1, 2, \ldots, 2^{2s}-1 \, . \end{cases}$$

PROOF:

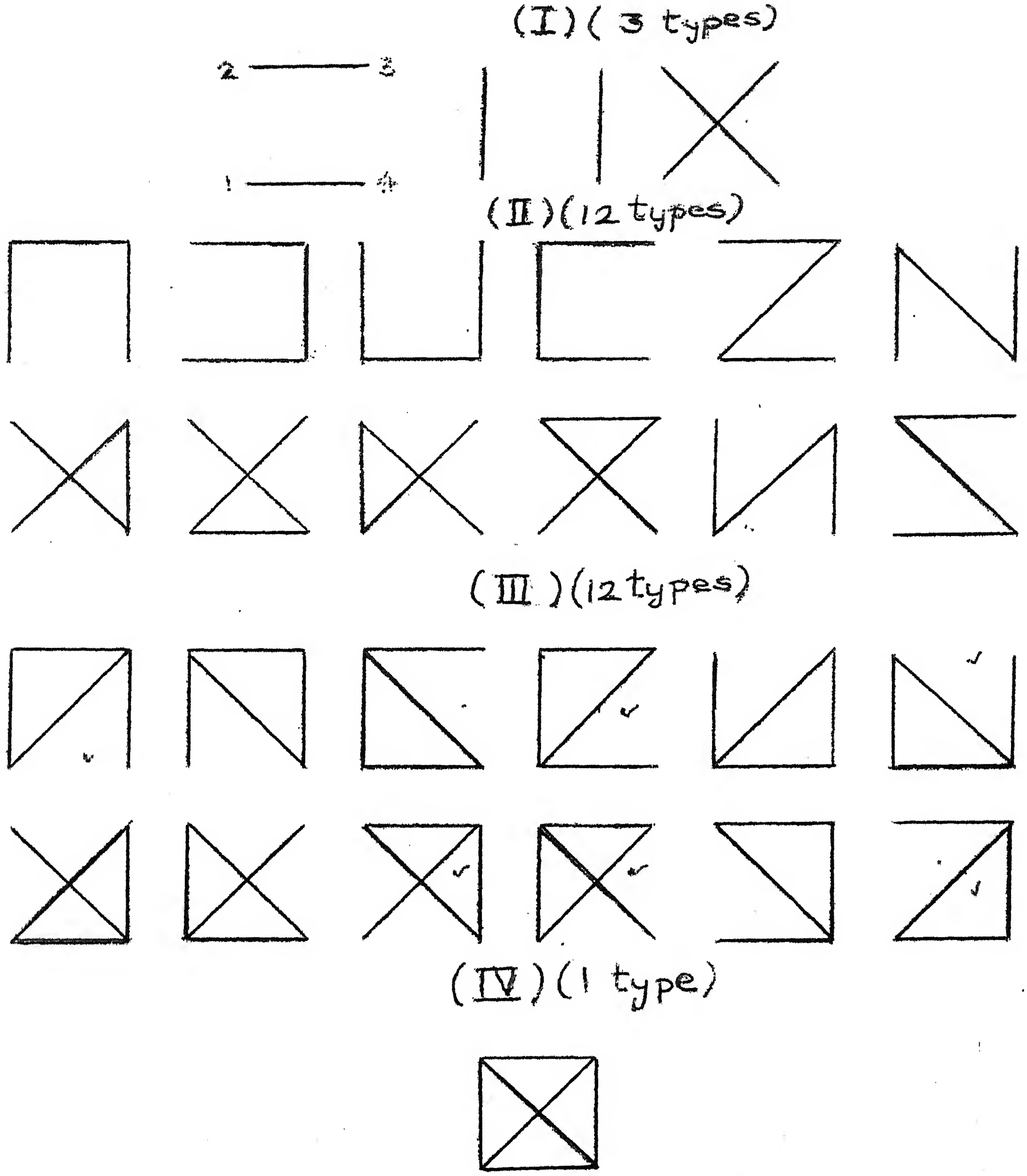
(i) Let f(v) be a bent function of $m = 2s$ variables

$$\underline{F} = \underline{\underline{H}}\ {}^{c}\underline{f}$$

So, $F(i) = \pm\ 2^{s}$, $i = 0, 1, \ldots 2^{2s}-1$.

Now $\underline{b}_f = 2^{2s}.\underline{\underline{H}}\,(\frac{1}{2^{2s}} \underline{F} \cdot \frac{1}{2^{2s}} \underline{F}\,)$

Table 5.3



(I) (3 types)

(II) (12 types)

(III) (12 types)

(IV) (1 type)

$$\text{So,}\quad \underline{b}_f = \frac{1}{2^{2s}} \cdot \underline{\underline{H}} \cdot \left[2^{2s} \ldots\ldots\ 2^{2s}\right]^T$$

$$= \underline{\underline{H}} \cdot \left[1\ 1 \ldots\ldots 1\right]^T$$

$$\text{Thus,}\quad b_f(t) = \begin{cases} 2^{2s} & , \ t = 0 \\ 0 & , \ t = 1, 2, \ldots, 2^{2s-1} \end{cases} .$$

(ii) Let $f(v)$ be a Boolean function of $m = 2s$ variables with dyadic auto-correlation of the type given above.

$$\text{So,}\quad \left[2^{2s}\ 0 \ldots\ldots 0\right]^T = \frac{1}{2^{2s}} \underline{\underline{H}}\ \underline{F}^2$$

$$\text{Or,}\quad \underline{F}^2 = 2^{2s}\ \underline{\underline{H}}^{-1}\ \underline{b}_f$$

$$= \underline{\underline{H}}\ \underline{b}_f$$

$$= \left[2^{2s} \ldots\ldots 2^{2s}\right]^T$$

So, each $F_i = \pm\ 2^s$,

Hence, $f(v)$ is a bent function.

Q.E.D.

CHAPTER 6

CONCLUSION

We began with an integrated approach to correlation, linear systems and the system-specfic transforms. Design of signals with good correlation properties is posed as an important problem within this overall perspective. Sequences with ideal and asymptotically-ideal cyclic correlation properties have been reviewed from the linear cyclic-shift invariant (LCSIV) systems' and discrete Fourier transform (DFT) points of view, thus, establishing necessary and sufficient conditions for any sequences to possess these properties. In fact, these results expound criteria which aid the synthesis of generalised sequences with desired correlation properties. However, binary sequences were dwelled upon more because of their obvious advantages in terms of generation and other properties.

We passed on, further, to an exposition of the interrelations between linear dyadic-shift invariant (LDSIV) systems, dyadic correlation and the Walsh-Hadamard transform, thus, preparing the groundwork for a study of sequences with good dyadic correlation properties. Non-repetitive quadratic forms (NRQFs), a class of binary Boolean functions, was dealt with extensively as a set of binary sequences with ideal and asymptotically ideal auto- and cross-correlation properties, respectively. The uniform-magnitude Walsh-Hadamard transform of NRQFs was arrived at in a general way, and applied to their generalise dyadic correlation analysis. This approach lead to some interesting results. In order to assess the periodic and aperiodic correlation performance of NRQFs, periodic and aperiodic correlation parameters were computed for some specific cases and compared with those of m-sequences.

We also presented an integrated brief overview of bent functions, a larger class (than NRQFs) of binary functions with uniform-magnitude sequency-spectrum and hence, the ideal dyadic auto-correlation property. The uniform-magnitude spectral property suggests a method to obtain generalised bent functions. These were also presented. The generalised bent functions constitute a complete set with ideal dyadic auto-correlation. This important observation marked the end of dyadic correlation analysis attempted in this work.

6.1 SCOPE FOR FURTHER WORK

Two problems related to the present work which have been investigated summarily are dealt with presently. First is the design of binary sequences with specified dyadic auto-correlations using the method of dyadic difference sets. This is analogous to the synthesis of sequences with specified cyclic correlations using integer difference sets. The problem is introduced here, a detailed analysis being beyond the scope of this work. Section 6.1.1 introduces the method for cyclic sequences which is extended to that for the dyadic case in Section 6.1.2.

Another problem of interest is the study of dyadic correlation properties of 2-D arrays. It is introduced in Sec.6.1.3. Sections 6.1.4 and 6.1.5 present two methods of synthesis of 2-D arrays from 1-D binary sequences. Some interesting results are derived with NRQFs and Walsh functions as the 1-D component arrays.

6.1.1 Integer Differences Sets and Periodic Correlation

Let $\underline{x} = (x_o x_1 \ldots x_{N-1})$ be a $\{0,1\}$ N-length sequence with k ones. The out-of-phase periodic auto-correlation is:

$$A(t) = \sum_{i=0}^{N-1} (-1)^{x_i} (-1)^{x_{i-t}} , \quad t = 1,2,\ldots (N-1), \quad (i-t) \bmod N.$$

Let A be a constant for all t as is the case with pseudo-random sequences. Define m to be the number of places, in which $\{x_i\}$ and $\{x_{i-t}\}$ have a one in common i.e.,

$x_i = x_{i-t} = 1$ for exactly m values of i, $0 \leqslant i \leqslant N-1$

and for all t, $1 \leqslant t \leqslant N-1$.

So, the arrangement of ones and zeros of $\{x_i\}$ and $\{x_{i-t}\}$ is as follows:

$$\begin{array}{rcccc} & m & (k-m) & (k-m) & N-m-2(k-m) \\ x_i & \overline{1\ldots\ldots1} & \overline{1\ldots\ldots1} & \overline{0\ldots\ldots0} & \overline{0\ldots\ldots\ldots\ldots\ldots0} \\ x_{i-t} & 1\ldots\ldots1 & 0\ldots\ldots0 & 1\ldots\ldots1 & 0\ldots\ldots\ldots\ldots\ldots0 \end{array}$$

Thus, $A = m(-1)^1(-1)^1 + 2(k-m)(-1)^1(-1)^0 + (N-2k+m)$

$$= m - 2k + 2m + N - 2k + m$$

$$= N-4k+4m$$

For a given N and k, A is constant if there are exactly m overlapping ones between $\left\{x_i\right\}$ and $\left\{x_{i-t}\right\}$, for all t.

This is possible if each non-zero cyclic shift, t, is expressible as a difference mod N between each of exactly m pairs of numbers mod N, each number being i such that $x_i = 1$.

<u>Example 6.1</u>: Let $\underline{x}$ be a 7-length sequence:

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}, \quad k=4$$

It is to be noted that

t	Differences
1	(0-6), (6-5)
2	(0-5), (5-3)
3	(3-0), (6-3)
4	(3-6), (0-3)
5	(5-0), (3-5)
6	(6-0), (5-6)

Numbers in each pair constitute the set $\left\{0, 3, 5, 6\right\}$, every element of which is an i such the $x_i = 1$ in $\underline{x}$.

The problem of synthesizing sequences with given N,k and A is related to the existence of integer difference sets with parameters (N, k, m).

Integer Difference Sets [Meetham, 1969]:

A set of k distinct integers $(d_1, d_2, \ldots, d_k)$ modulo an integer N is called an integer difference set D with parameters (N, K, m), if every integer $b \not\equiv 0 \pmod N$ can be expressed in exactly m ways in the form $d_i - d_j \equiv b \pmod N$, where d_i, d_j belong to D.

Hence, if for desired A, k and m, such a difference set is found, then the sequence with out-of-phase auto-correlation A can be formed.

Example 6.2: Consider a 7-length sequence. A is desired to be -1.

So, $-1 = N - 4k + 4m$.

Choosing $k = 4$, $m = 2$

There exists a difference set, D, mod 7 with parameters (7,4,2). If $D = \{0, 3, 4, 5\}$ with mod 7,

$$\text{then} \quad \left.\begin{array}{l} 1 \equiv 4 - 3 \equiv 5 - 4 \\ 2 \equiv 5 - 3 \equiv 0 - 5 \\ 3 \equiv 3 - 0 \equiv 0 - 4 \\ 4 \equiv 0 - 3 \equiv 4 - 0 \\ 5 \equiv 3 - 5 \equiv 5 - 0 \\ 6 \equiv 3 - 4 \equiv 4 - 5 \end{array}\right. \quad \text{mod } 7$$

Assigning a '1' to position numbers in D and '0' to the rest we get,

$$\begin{array}{ccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \underline{x} & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}$$ which has the desired correlation:

$7\ -1\ -1\ -1\ -1\ -1\ -1$.

Hence, each such D with parameters (N, k, m) corresponds to a binary sequence with out-of-phase auto-correlation (N-4k-4m).

6.1.2 Dyadic Difference sets and Dyadic Correlation

Let $\underline{x}=(x_o\ldots x_{N-1})$, where $N=2^n$, be a binary $\{0,1\}$ sequence.

$$b(t)=\sum_{i=0}^{N-1}(-1)^{x_i}(-1)^{x_{i\oplus t}}\ ,\ t=1,2,\ldots,(N-1)$$

is the out-of-phase dyadic auto-correlation. Again, let k be the ones in $\underline{x}$ and m be the number of places in which $\{x_i\}$ and its dyadic shifted version $\{x_{i\oplus t}\}$ have a one in common for all t, $1\leqslant t\leqslant(N-1)$.

So, $b(t)=N-4k+4m$.

For desired b, N and k, a difference set with mod 2 ($\oplus$) as the operation is required such that each $i\not\equiv 0$ (mod N) can be represented in exactly m ways as the $\oplus$ sum of pairs of its elements.

Dyadic Difference Set:

A set of k distinct field elements $\{d_1, \ldots. d_k\}$ over a finite field of N elements is called a dyadic difference set, D, with parameters (N, k, m) if every field element $b\not\equiv 0$ can be expressed in exactly m ways in the form $d_i\oplus d_j\equiv b$, where d_i, d_j belong to D.

One possible way of choosing a finite field of N elements to represent position numbers from 0 to (N-1), with $\oplus$ as the operation, is using primitive irreducible polynomial over GF(2) of degree n $(N = 2^n)$. This generates an extension field $GF(2^n)$ with $\oplus$ as the field operation.

Example 6.3: As an illustrative example, let $N = 2^4 = 16$. Use the degree 4 primitive polynomial

$$z^4 = z \oplus 1 \text{ to generate the field.}$$

Let a be the primitives element.

So, $a^4 = a \oplus 1$.

All the field elements, their chosen binary representation and the position numbers they represent are as follows:

Field Element	Binary Representation	Position Numbers
0	0000	0
$1 = a^{15}$	0001	1
a	0010	2
a^2	0100	4
a^3	1000	8
$a^4 = a \oplus 1$	0011	3
$a^5 = a^2 \oplus a$	0110	6
$a^6 = a^3 \oplus a^2$	1100	12
$a^7 = a^3 \oplus a \oplus 1$	1011	11
$a^8 = a^2 \oplus 1$	0101	5
$a^9 = a^3 \oplus a$	1010	10
$a^{10} = a^2 \oplus a \oplus 1$	0111	7
$a^{11} = a^3 \oplus a^2 \oplus a$	1110	14

..contd.

$a^{12} = a^3 \oplus a^2 \oplus a \oplus 1$	1111	15
$a^{13} = a^3 \oplus a^2 \oplus 1$	1101	13
$a^{14} = a^3 \oplus 1$	1001	9

For ideal auto-correlation, $b(t) = 0$ and let $k = 6$ if $N = 16$ (taking a cue from bent functions).

So, $0 = 16 - 4\ (6) + 4\ m$

or $m = 2$.

Thus, a dyadic difference set with six elements is to be chosen such that all the non-zero field elements are expressible as $\oplus$ sum of pairs of its members in exactly two ways.

One of the possible choices is:

$$D = \left\{a^5, a^{10}, a^7, a^{14}, a^{13}, a^{11}\right\}$$

It can be verified that:

$$1 = a^{15} = a^5 \oplus a^{10} = a^{10} \oplus a^5$$

$$2 = a = a^{14} \oplus a^7 = a^7 \oplus a^{14}$$

$$3 = a^4 = a^{13} \oplus a^{11} = a^{11} \oplus a^{13}$$

$$4 = a^2 = a^{14} \oplus a^{13} = a^{13} \oplus a^{14}$$

$$5 = a^8 = a^7 \oplus a^{11} = a^{11} \oplus a^7$$

$$6 = a^5 = a^7 \oplus a^{13} = a^{13} \oplus a^7$$

$$7 = a^{10} = a^{11} \oplus a^{14} = a^{14} \oplus a^{11}$$

$$8 = a^3 = a^5 \oplus a^{11} = a^{11} \oplus a^5$$

$$9 = a^{14} = a^{10} \oplus a^{11} = a^{11} \oplus a^{10}$$

$$10 = a^9 = a^{10} \oplus a^{13} = a^{13} \oplus a^{10}$$

... contd.

$$
\begin{aligned}
11 &= a^7 &&= a^5 \oplus a^{13} &&= a^{13} \oplus a^5 \\
12 &= a^6 &&= a^7 \oplus a^{10} &&= a^{10} \oplus a^7 \\
13 &= a^{13} &&= a^5 \oplus a^7 &&= a^7 \oplus a^5 \\
14 &= a^{11} &&= a^{10} \oplus a^{14} &&= a^{14} \oplus a^{10} \\
15 &= a^{12} &&= a^5 \oplus a^{14} &&= a^{14} \oplus a^5
\end{aligned}
$$

Assigning a '1' to the position numbers corresponding to the elements of D and a '0' to the rest, we get the sequence:

0	a^{15}	a	a^4	a^2	a^8	a^5	a^{10}	a^3	a^{14}	a^9	a^7	a^6	a^{13}	a^{11}	a^{12}
0	0	0	0	0	0	1	1	0	1	0	1	0	1	1	0

This has '0' out-of-phase dyadic auto-correlation as desired. Incidentally, this is also an NRQF : $f(\underline{x}) = x_1x_4 \oplus x_2x_3$.

This outline suggests that if dyadic difference sets with parameters (N, k, m) can be constructed, then sequences with desired dyadic auto-correlation can be designed. Using GF(2^n) as the finite field, all the primitive degree n polynomials have to be tried. Another method outlined by [McFarland, 1973] can also be tried. There can be many dyadic difference sets arising out of a given degree n primitive polynomial. This also suggests a possible method for enumeration of bent functions of n variables. Each dyadic difference set with (N, k, m) such that $b(t) = 0$, $t = 1, \ldots (N-1)$ and $k = 2^{n-1} - 2^{n/2-1}$ represents a binary sequence which is a bent function. In other words, there is a one-to-one correspondence between such difference sets and bent functions.

6.1.3 Dyadic Correlation Properties of two-Dimensional Arrays

Let $C(x,y)$ and $D(x,y)$ be two $N \times M$ $(N = 2^n,\ M = 2^m)$ 2-dimensional (2-D) real-valued arrays. Dyadic correlation, $R_{CD}\,(i,j)$, is expressed as:

$$R_{CD}\,(i,j) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} C(x,y)\ D(x \oplus i,\ y \oplus j)$$

$$i = 0, 1, \ldots, (N-1),$$

$$j = 0, 1, \ldots, (M-1)$$

If $C(x,y) = D(x,y)$,

$$R_C\,(i,j) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} C(x,y)\ C(x \oplus i,\ y \oplus j).$$

Nature of the correlation function, $R(i,j)$, depends on the method used for construction of the 2-D arrays [Calabro and Wolf, 1967]. The obvious choice falls on 1-D arrys having good correlation properties as basis of extension to the 2-D case. Two methods of forming binary 2-D arrays are discussed with examples using NRQFs and Walsh functions as building blocks. NRQFs are taken to be $\{+1,-1\}$ - valued.

6.1.4 2-D Arrays from Dyadic Shifts of 1-D Arrays

Let, $f(u)$ and $g(u)$ be two N-point $(N = 2^n)$ $\{+1,\ -1\}$-valued functions. Consider two 2-D arrays, $C(x,y)$ and $D(x,y)$, constructed as follows:

$$C(x,y) = f(x \oplus y) \quad ,$$

$$D(x,y) = g(x \oplus y) \quad , \text{ C and D are both } N \times N .$$

$$R_C(i,j) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(x,y)\ C(x \oplus i,\ y \oplus j)$$

$$= \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x \oplus y)\ f(x \oplus y \oplus i \oplus j)$$

$$= \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} f(z)\ f(z \oplus i \oplus j),\quad z = x \oplus y$$

$= N\ b_f(i \oplus j)$, where $b_f(t)$ is the dyadic auto-correlation function of $f(x)$.

Rows of $\underline{\underline{R}}_C$ are dyadic shifts of $b_f(t)$.

(i) If $f(x)$ is chosen to be an NRQF,

$$b_f(t) = N\,\delta_{t0}\ ,\ \text{and}$$

$$R_C(i,j) = N.N\,\delta_{i \oplus j,0}$$

$$= N^2\,\delta_{ij}$$

$R_C(i,j)$ is a diagonal matrix with this choice of $f(x)$.

(ii) If $f(x)$ is chosen to be $\underline{H}_k$, the kth row of $\underline{\underline{H}}$ (the N x N Hadamard matrix), then,

$$\underline{b}_{\underline{H}_k} = N\ \underline{H}_k\ .$$

So, $R_C(i,j) = N.N.h_{k,i \oplus j}$

$$= N^2\ h_{ki}\ h_{kj}$$

$$= \pm\ N^2$$

$$R_{CD}(i,j) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x,y)\ D(x \oplus i,\ y \oplus j)$$

$$= \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x \oplus y)\ g(x \oplus y \oplus i \oplus j)$$

$$= \sum_{x=0}^{N-1}\sum_{z=0}^{N-1} f(z)\ g(z \oplus i \oplus j)\ ,\ z = x \oplus y$$

$$= N\ b_{fg}\ (i \oplus j)$$

(i) Let $f(x)$ and $g(x)$ be NRQFs. Then, rows of $\underline{\underline{R}}_{CD}$ are dyadic shifts of $b_{fg}(t)$. Each row will have that many non-zero values as $b_{fg}(t)$.

<u>Example 6.4</u>: Let $f(x) = x_1x_2 \oplus x_3x_4$ and

$g(x) = x_1x_3 \oplus x_2x_4$. $N = 2^4 = 16$

$$b_{fg}(t) = \begin{cases} 8\ , & t = 0,\ 6,\ 9 \\ -8\ , & t = 15 \\ 0\ , & \text{otherwise} \end{cases}$$

Dyadic shifts (i,j), for which $R_{CD}(i,j)$ is non-zero are given in Table 6.1. Figures in parentheses are the correlation values (normalised).

(ii) Let $\underline{f} = \underline{H}_k$ and $\underline{g} = \underline{H}_q$ be the choice of $\underline{f}$ and $\underline{g}$. It is known that dyadic cross-correlation function between two Walsh functions is identically equal to zero.

i.e. $b_{fg}(t) = 0$, for all t.

So, $R_{CD}(i,j) = 0$, for all i and j which is similar to the ideal cross-correlation for 1-D arrays.

Table 6.1

$j = i \oplus t$

t i	0 (8)	6 (8)	9 (8)	15 (-8)
0	0	6	9	15
1	1	7	8	14
2	2	4	11	13
3	3	5	10	12
4	4	2	13	11
5	5	3	12	10
6	6	0	15	9
7	7	1	14	8
8	8	14	1	7
9	9	15	0	6
10	10	12	3	5
11	11	13	2	4
12	12	10	5	3
13	13	11	4	2
14	14	8	7	1
15	15	9	6	0

(iii) Consider $\underline{f} = \underline{H}_k$ and $g(x)$, an NRQF, as the next choice

$$b_{fg}(t) = \pm \ (N)^{\frac{1}{2}}$$

Hence, $R_{CD}\ (i,j) = \pm \ (N)^{3/2}$

$$= \pm \ (2^{3s}) \ , \ N = 2^{2s}$$

6.1.5 2-D Arrays as Termwise Product of 1-D Arrays

2-D arrays can be constructed from term-by-term product of 1-D arrays. Consider, $A(x,y)$, an $N \times M$ ($N = 2^n$, $M = 2^m$) array formed using an N-length array $C(x)$ and an M-length one, B(y) such that:

$$A(x,y) = C(x)\ D(y)$$

Then, $R_A(i,j) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} A(x,y)\ A(x \oplus i,\ y \oplus j)$

$$= \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(x)\ D(y)\ C(x \oplus i)\ D(y \oplus j)$$

$$= b_C(i)\ b_D(j).$$

$R_A(i,j)$ is the termwise product of auto-correlations of C(x) and D(y).

(i) If C(x) and D(u) are N- and M-point NRQFs,

$$b_C(i) = N\ \delta_{i0},$$
$$b_D(j) = M\ \delta_{j0}$$

Hence, $R_A(i,j) = NM\ \delta_{(i,j),(0,0)}$ i.e. it is zero for all non-zero shifts. This is similar to the ideal auto-correlation property of 1-Darrays.

(ii) If C(x) and D(y) are N- and M-point Walsh functions,

$$R_A(i,j) = (\pm N).(\pm M) \text{ for all } i,j.$$
$$= \pm\ NM.$$

(iii) C(x), an N-point NRQF, and D(x), an M-point Walsh function, is another choice.

Then, $R_A(i,j) = N\ \delta_{i0}.(\pm\ M)$

$$= \pm\ NM\ \delta_{i0}$$

REFERENCES

1) [Ahmed and Rao, 1975]: N. Ahmed and K.R. Rao, Orthogonal Transforms for digital signal processing, Berlin, Springer-Verlag, 1975.

2) [Boehmer, 1967]: A.M. Boehmer, "Binary Pulse Compression Codes," IEEE Trans. Inform. Theory, vol. IT-13, pp. 156-167, 1967.

3) [Calabro and Wolf, 1967]: D. Calabro and J.K. Wolf, "On the Synthesis of 2-D Arrays with Desirable Correlation Properties," Information and Control, 11, pp. 537-560, 1968.

4) [Chu, 1972] : D.C. Chu, "Polyphase Codes with good periodic Correlation properties," IEEE Trans. Inform. Theory, vol.IT-18, pp. 521-532, 1972.

5) [Fiestal et al., 1975]: Fiestal et al., "Some Cryptographic techniques for m/c-to-m/c data communications," Proc. IEEE, vol. 63, pp. 545-54, 1975.

6) [Frank and Zadoff, 1962]: R. Frank and S. Zadoff, "Phase shift Codes with good periodic correlation properties," IRE Trans. Inform. Theory, vol. IT- 8, pp. 381-382, 1962.

) [Geffe, 1973]: P.R. Geffe, "How to protect data with ciphers that are really hard to break," Electronics, vol. 46, pp.99-101, 1973.

8) [Golomb, 1967] : S.W. Golomb, Shift Register Sequences, San Francisco, CA: Holden-Day, 1967.

9) [Golomb, 1964] : S.W. Golomb, Ed., Digital Communications with Space Applications, Englewood Cliffs, NJ: Prentice Hall, 1964.

10) [Golomb and Scholtz, 1965]: S.W. Golomb and R.A. Scholtz, "Generalised Barker Sequences," IEEE Trans. Inform. Theory, vol. IT-11, pp. 533-537, 1965.

12) [Henriksson, 1972]: Henriksson, "On a scrambling property of shift registers," IEEE Trans. Comm., COM-20, pp. 998-1001, 1972.

12) [Huffman, 1962]: D.A. Huffman, "The generation of impulse-equivalent pulse trains," IRE Trans. Inform. Theory, vol.IT-8 pp. S10-S16, 1962.

13) [Karpovsky, 1976]: M.G. Karpovsky, Finite Orthogonal series in the design of digital devices, N.Y. Wiley, 1976.

14) [Key, 1976]: E.L. Key, "Analysis of the structure and complexity of Nonlinear Binary Sequence Generators," IEEE Trans. Inform. Theory, vol. IT-22, pp. 732-736, 1976.

15) [MacWilliams and Sloane, 1976] : F.J. MacWilliams and N.J.A. Sloane, "Pseudo-random sequences and arrays," Proc. IEEE. vol. 64, pp. 1715-1729, 1976.

16) [MacWilliams and Sloane, 1977] : F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

17) [Massey, 1969]: J.L. Massey, "Shift-Register Synthesis and RCH decoding," IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, 1969.

18) [McFarland, 1973] : R.McFarland, "A family of difference sets in noncyclic groups," Journal of Combinatorial Theory (A), vol. 15, pp. 1-10, 1973.

19) [Meetham, 1969] : A.R. Meetham, Ed., Encyclopaedia of Linguistics, Information and Control, Pergamon Press, Oxford, pp. 420-421, 1969.

20) [Pursley and Sarwate, 1977]: M.B. Pursley and D.V. Sarwate, "Performance evaluation for phase-coded spread-spectrum multiple-access communication - Part II: Code-sequence analysis," IEEE Trans. Commun., vol. COM-25, pp. 800-803, 1977.

21) [Pursley and Roefs, 1979]: M.B. Pursley and H.F.A. Roefs, "Numerical evaluation of correlation parameters for optimal phases of binary-shift register sequences," IEEE Trans. Commn., vol. COM-27, pp. 1597-1604, 1979.

22) [Rothaus, 1976]: O.S. Rothaus, "On 'Bent' Functions," Journal of Combinatorial Theory (A), vol. 20, No. 3, pp. 300-305, 1976.

23) [Sarwate and Pursley, 1980]: D.V. Sarwate and M.B. Pursley, "Cross-correlation properties of Pseudorandom and related sequences," Proc. IEEE, vol. 68, pp. 593-619, 1980.

24) [Shedd and Sarwate, 1979]: D.A. Shedd and D.V. Sarwate, "Construction of sequences with good correlation properties," IEEE Trans. Inform. Theory, vol. IT-25, pp. 94-97, 1979.

25) [Taki and Miyakawa, 1969]: Taki and Miyakawa, "Even-shift orthogonal sequences," IEEE Trans. Inform. Theory, vol. IT-15, pp. 295-300, 1969.

APPENDIX-A

```
C*********************************************************************
C----  PROGRAM TO COMPUTE AUTO-OPTIMAL/LEAST SIDELOBE ENERGY   ----
C-----  PHASES OF M-POINT N-VARIABLE o-NROFs IN THEIR (1,-1)   ----
C------                      FORMS                          -------
C      -----------------------------------------------------
C
C---------------------------------------------------------------------
C------------------------------  LEGEND  -----------------------------
C-----  FI : REPRESENTATION OF NROF F IN TERMS OF ITS INDICES      ---
C-----  F IS CMPTD FROM FI AND CONVERTED TO FC ITS (1,-1)FORM      ---
C---  BCFG : APERIODIC AUTO-CORRELATION OF F                       ---
C---  OCFG : ODD AUTO-CORRELATION OF F                             ---
C----------  [REST OF THE VARS WITH THEIR CONTEXTS]  ----------------
C---------------------------------------------------------------------
C*********************************************************************
      INTEGER F(256),MODS,FC(256),BCFG(256),OCFG(256),FI(8)
      INTEGER MODD(256),L(256),S(256),A(256),LL(256)
      INTEGER LSI(256),MPOS(256),SS(256)
      COMMON LIMU
3000  CONTINUE
C---------------------------------------------------------------------
C
C
C------                    SETTING MPOS                      -------
C----  MPOS : ARRAY OF ALL PHASES FROM 0 TO M-1                  ----
C     ------------------------------------------------------
      DO 345 IK=1,M
345   MPOS(IK)=IK-1
C
C-----------  INPUT o-NROF IN FORM OF FI-ITS INDICES  -----------
C----  N : NUMBER OF VARIABLES                                  -----
C     ------------------------------------------------------
      ACCEPT *,N,(FI(I),I=1,N)
C
C------                  TERMINATION FLAG                    --------
C     ------------------------------------------------------
      IF(FI(1).EQ.-1)STOP
C
C----  CADNRO : CMPTES F IN (0,1)-FORM FROM FI AND N  -----------
C     ------------------------------------------------
      CALL CADNRO(F,FI,N)
C
      TYPE101,(FI(I),I=1,N)
101   FORMAT(1X,'FUNCTION F',12I3)
      TYPE1,((F(I),I=1,M))
1     FORMAT(1X,'FUNCTION F',256I2)
C
C------                 CONVERT F INTO FC                     ------
C     ------------------------------------------------------
      DO 400 I=1,M
400   FC(I)=1-2*F(I)
C
C
C
```

```
C------  THIS LOOP PHASE SHIFTS FC SUCCESSIVELY AND CMPTS  -----
C--------  MAX ODD CORR & NO. OF OCCURENCES FOR EACH PHASE  ----
C       -----------------------------------------------------------
      DO 111 IO=1,M
      IO=IO-1
      IF(IO.EQ.1)GOTO1001
C
C------                   PHASE SHIFT BY ONE                     ------
C      -----------------------------------------------------------
      IPD1=FC(1)
      DO 112 IL=1,M
      ILD=IL+1
      IF(ILD.GT.M)ILD=ILD-M
      ND1=FC(ILD)
      FC(ILD)=IPD1
      IPD1=ND1
112   CONTINUE
1001  CONTINUE
C----------------------------------------------------------------------
C
C------                      SETTING BCFG                        ------
C      -----------------------------------------------------------
      DO 100 I=1,M
100   BCFG(I)=0
C
C------                 CMPTING APERIODIC CORR                   ------
C      -----------------------------------------------------------
      DO 200 I=1,M
      DO 300 J=1,M
      JDUM=J-(I-1)
      IF(JDUM.LE.0)GOTO300
      BCFG(I)=BCFG(I)+FC(J)*FC(JDUM)
300   CONTINUE
200   CONTINUE
C----------------------------------------------------------------------
C
C------                 CMPTING ODD AUTO-CORR                    ------
C      -----------------------------------------------------------
      OCFG(1)=BCFG(1)
      MDUM=(M+2)/2
      DO 777 J1=2,MDUM
      J1D=M+2-J1
      OCFG(J1)=BCFG(J1)-BCFG(J1D)
      OCFG(J1D)=-(BCFG(J1)-BCFG(J1D))
777   CONTINUE
C
C------                 CMPTING MAX ODD CORR                     ------
C      -----------------------------------------------------------
      MEQ=M/2+1
C
C----  MAXCOR : CMPTES 'MAX' OCFG & NMAX, NO. OF OCCRNCS          -----
C----     MEQ : NO. OF OCFG's TO BE EXAMINED                      -----
C     -------------------------------------------------------------
      CALL MAXCOR(OCFG,MEQ,MAX,NMAX)
      IF(ABS(OCFG(MEQ)).EQ.ABS(MAX))GOTO534
      NMAX=NMAX*2
      GOTO5345
534   NMAX=(NMAX-1)*2+1
5345  CONTINUE
C----------------------------------------------------------------------
```

```
C
C------            SETTING MODD,L AND S
C------   MODD : ARRAY OF MAX ODD CORR FOR EACH PHASE          -----
C------      L : ARRAY OF NO. OF OCCRNCS OF MODD               -----
C------      S : ARRAY OF SIDELOBE ENERGIES                    -----
C     ---------------------------------------------------------------
      MODD(ID)=ABS(MAX);L(ID)=NMAX;S(ID)=0
      DO 33 JL=2,N
33    S(ID)=S(ID)+BCFG(JL)**2
C--------------------------------------------------------------------------
111   CONTINUE
C
C-------- CMPTATION OF MODD,L & S FOR EACH PHASE ENDS  --------
C         ---------------------------------------------
C
C---------- CMPTE MIN OF THE MODD OVER ALL PHASES  ----------
C           ----------------------------------------
      LIMU=N
C
C----  MINMAX : CMPTES MIN OF MODD AND NO. OF OCCRNCS          ----
C----       A : ARRAY PHASES FOR WHICH MODD IS A MIN           ----
C----       J : NO. OF SUCH PHASES                             ----
C----     MIN : MIN ODD CORR                                   ----
C    -----------------------------------------------------------
      CALL MINMAX(MODD,NPOS,A,J,2, MIN)
      IF(J.EQ.1)GOTO2222
C--------------------------------------------------------------------------
C
C-------- CMPTE LEAST L PHASE(S) OF MIN MODD PHASES  --------
C         -------------------------------------------
      LIMU=J
C
C----      LL : PHASE(S) WITH LEAST L & MIN MODD               ----
C----       K : NO. OF SUCH PHASE(S)                           ----
C----    MINL : MIN OCCURENCE                                  ----
C    -----------------------------------------------------------
      CALL MINMAX(L,A,LL,K,2, MINL)
      IF(K.EQ.1)GOTO2223
C
C------ SETTING ARRAY SS AS SLEs OF MINL & MIN MODD PHASES  ------
C       ----------------------------------------------------
      IN=0
      DO 450 I=1,K
      IN=IN+1
      LID=LL(I)+1
450   SS(IN)=S(LID)
C--------------------------------------------------------------------------
C
C---- CMPTING LEAST SLE PHASE(S) OF MINL & MIN MODD PHASE(S)  ---
C----------------- THESE ARE THE AO/LSE PHASE(S)  ----------------
C                  -----------------------------
      LIMU=K
C
C----     LSI : AO/LSE PHASE(S)                                ----
C----      K1 : NO.OF AO/LSE PHASS(S)                          ----
C----    MINS : LSE                                            ----
C    -----------------------------------------------------------
      CALL MINMAX(S,LL,LSI K1,2, MINS)
      TYPE91,(LSI(I),I=1,K1)
91    FORMAT(1X,'**OPT PHASE(S)**',64I4)
```

```
      TYPE92,MIN,MINL,MINS
92    FORMAT(1X,'***ODDCORMINMAX  =',I4,'  ***',/
     1       1X,'*NO OF OCCURENCES=',I4,'  ***',/
     2       1X,'*SIDELOBE ENERGY =',I5,' ***')
      GOTO245
C-----------------------------------------------------------------------
2222  LA=A(1)+1
      TYPE44,A(1),MIN,L(LA),S(LA)
44    FORMAT(1X,'***OPTIMAL PHASE IS   ',I4,'  ***',/
     1       1X,'******ODDCOR   MAX   =',I4,'  ***',/
     2       1X,'**NO OF OCCURENCES   =',I4,'  ***',/
     3       1X,'***SIDELOBE ENERGY   =',I5,' ***')
      GOTO245
C-----------------------------------------------------------------------
2223  LLL=LL(1)+1
      TYPE44,LL(1),MODD(LLL),MINL,S(LLL)
245   CONTINUE
      GOTO3000
      STOP
      END
C-----------------------------------------------------------------------
C
C<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
C-----------------------  SUBROUTINES  --------------------------
C<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
C
C*************  MAXCOR COMPUTES MAXIMA OF AN ARRAY  *************
C----       A : GIVEN ARRAY                                      ----
C----      ML : LENGTH OF ARRAY A                                ----
C----     MAX : MAXIMA                                           ----
C----    NMAX : CARDINALITY OF THE MAXIMA SET                    ----
C      ******************************************************
      SUBROUTINE MAXCOR(A,ML,MAX,NMAX)
      INTEGER A(256)
      COMMON LIMU
      NMAX=0;MAX=0
      DO 100 I=2,ML
      IF(ABS(A(I)).LT.ABS(MAX))GOTO100
      IF(ABS(A(I)).EQ.ABS(MAX))GOTO1000
      MAX=A(I);NMAX=1
      GOTO100
1000  NMAX=NMAX+1
100   CONTINUE
      RETURN
      END
C-----------------------------------------------------------------------
C
C**************  MINMAX CMPTES MIN OF AN ARRAY  **************
C----  MIMO : GIVEN ARRAY                                   ----
C----    NP : ARRAY POINTS WHOSE MIN IS TO BE CMPTED        ----
C----   NPN : ARRAY POINTS WHERE MINIMA OCCURS              ----
C----   NNP : NO. OF MIN POINTS                             ----
C----  LLIM : STARTING POINT OF SEARCH                      ----
C----   MIM : THE MINIMA                                    ----
C      *********************************************
       SUBROUTINE MINMAX(MIMO,NP,NPN,NNP,LLIM, MIM)
       INTEGER MIMO(256),NP(256),NPN(256)
       COMMON LIMU
       LO=NP(1)+1;MIM=MIMO(LO);NNP=1;NPN(NNP)=LO-1
       DO 35 LK=LLIM,LIMU
      LD=NP(LK)+1
      IF(NIMO(LD).GT.NIM)GOTO36
      IF(NIMO(LD).EQ.NIM)GOTO334
      NIM=NIMO(LD)
      DO 37 LI=1,NNP
37    NPN(NNP)=0
      NNP=1
      NPN(NNP)=LD-1
      GOTO36
334   NNP=NNP+1
      NPN(NNP)=LD-1
36    CONTINUE
      RETURN
      END
C-----------------------------------------------------------------------
C
C**********************************************************************
C----  CALNRQ : COPUTES N-VAR Q-NROF FROM INDEX REPRESENTATION  -
C----        F : CMPTED NROF F IN (0,1)-FORM                    ----
C----        J : INDEX REP OF F                                 ----
C----        N : NO. OF VARS                                    ----
C    ***************************************************************
      SUBROUTINE CALNRQ(F,J,N)
       INTEGER F(256),BI(8),J(12)
      M=2**N
      DO 300 I=1,N
300   BI(I)=0
      DO 100 I=1,M
100   F(I)=0
      DO 200 I=1,M
      IDUM=I-1
      CALL BCONV(IDUM,BI,N)
               DO 400 K=1,N
      IF(J(K).GT.0)GOTO400
      JDUM=ABS(J(K))
      BI(JDUM)=1-BI(JDUM)
400   CONTINUE
      DO 200 K=1,N,2
      JDUM1=ABS(J(K))
      JDUM2=ABS(J(K+1))
      F(I)=(F(I)-BI(JDUM1)*BI(JDUM2))**2
200   CONTINUE
      RETURN
      END
C-----------------------------------------------------------------------
C**********************************************************************
C----  BCONV : CONVERTS C INTO N-BIT BINARY REP                 ----
C    ***************************************************************
      SUBROUTINE BCONV(C,BC,N)
      INTEGER C,BC(8),DUMC
      DO 10 I=1,N
      DUMC=C/2
      BC(I)=C-2*DUMC
10    C=DUMC
      RETURN
      END
C**********************************************************************
```

APPENDIX-B

```
C ****************************************************************
C----------  TO COMPUTE APERIODIC & PERIODIC CORRELATION  ---------
C----------  BETWEEN AD/LSE PHASED M-POINT p-NROFS F & G  ---------
C         ----------------------------------------------------
C
C------------------------------  LEGEND  -------------------------
C-----   F & G ARE N-VAR M-POINT p-NROFs READ IN THEIR INDEX  ---
C-----                  FORMS FI AND GI                       ---
C----   ECFG & ECGF : EVEN CORR BETWEEN F & G AND G & F       ---
C----   OCFG & OCGF :  ODD CORR BETWEEN F & G AND G & F       ---
C****************************************************************
C
      INTEGER F(256),G(256),MODS,FC(256),GC(256),BCFG(256)
      INTEGER BCGF(256),FI(8),GI(8),OCFG(256),ECFG(256)
      INTEGER FCS(256),GCS(256)
      COMMON LEND
C
3000  CONTINUE
C
C-----               INPUT FI AND GI                    -----
C-----              AND CMPTE F AND G                   -----
C----  ISHF & ISHG : AD/LSE PHASES OF F AND G           -----
C    ------------------------------------------------
      ACCEPT *,N,(FI(I),I=1,N),ISHF
      IF(FI(1).EQ.-1)STOP
      CALL CALARO(F,FI,N)
      ACCEPT*,N,(GI(I),I=1,N),ISHG
      CALL  CALARO(G,GI,N)
      TYPE101,(FI(I),I=1,N)
101   FORMAT(1X,'FUNCTION F',12I3)
      TYPE102,(GI(I),I=1,N)
102   FORMAT(1X,'FUNCTION G',12I3)
C--------------------------------------------------------------
C
C-----          CONVERT F & G INTO (1,-1)-FORM            -----
C      ------------------------------------------------
      DO 400 I=1,M
      FC(I)=1-2*F(I)
      GC(I)=1-2*G(I)
400   CONTINUE
C--------------------------------------------------------------
C
C-----       PHASING F & G INTO THEIR AD/LSE PHASES       -----
C      ------------------------------------------------
      IF(ISHF.EQ.0)GOTO222
      CALL CYSHIF(FC,M,ISHF,FCS)
222   CONTINUE
      IF(ISHG.EQ.0)GOTO223
      CALL CYSHIF(GC,M,ISHG,GCS)
223   CONTINUE
```

```
      DO 990 I7=1,M
      FC(I7)=FCS(I7)
      GC(I7)=GCS(I7)
990   CONTINUE
      ISHF=M-ISHF;ISHG=M-ISHG
      TYPE25,ISHF,ISHG
25    FORMAT(1X,'***FUNC FC CYCLICALLY SHIFTED BY',I3,'***',/
     1       1X,'***FUNC GC CYCLICALLY SHIFTED BY',I3,'***')
566   CONTINUE
C--------------------------------------------------------------------------
C                                                                    -----
C                          SETTING BCFG &BCGF
C-----                                                                   
C-    ---------------------------------------------------------------------
      DO 100 I=1,M
      BCFG(I)=0;BCGF(I)=0
100   CONTINUE
C--------------------------------------------------------------------------
C                                                                    -----
C                          COMPUTING BCFG & BCGF
C-----  ----------------------------------------------------------------
C      -----------------------------------------------------------------
      DO 200 I=1,M
      DO 300 J=1,M
      JDUM=J-(I-1)
      IF(JDUM.LE.0)GOTO300
      BCFG(I)=BCFG(I)+GC(J)*FC(JDUM)
      BCGF(I)=BCGF(I)+FC(J)*GC(JDUM)
300   CONTINUE
200   CONTINUE
C--------------------------------------------------------------------------
C                                                                    -----
C                          CMPTE MAX PER CORRELATION
C-----  ----------------------------------------------------------------
C      -----------------------------------------------------------------
      CALL MAXCOR(BCFG,M,MAX,NMAX)
      TYPE51,MAX,NMAX
51    FORMAT(1X,'***MAX LINCOR SIDELOBE=',I4,' ***',10X,
     1 '***NO OF OCCURENCES=',I4,'  ***')
C--------------------------------------------------------------------------
C                                                                    -----
C                          CMPTE ODD & EVEN CORR
C-----  ----------------------------------------------------------------
C      -----------------------------------------------------------------
      BCFS(1)=BCFG(1);ECFG(1)=BCFG(1)
      NDUM=(M+2)/2
      DO 777 J1=2,NDUM
      J1D=M+2-J1
      BCFS(J1)=BCFG(J1)-BCGF(J1D)
      BCFS(J1D)=-(BCGF(J1)-BCFG(J1D))
      BCFG(J1)=BCFG(J1)+BCGF(J1D)
      BCFG(J1D)=BCGF(J1)+BCFG(J1D)
777   CONTINUE
C--------------------------------------------------------------------------
C                                                                    -----
C                          CMPTE MAX EVE CORR
C-----  ----------------------------------------------------------------
C      -----------------------------------------------------------------
      MED=M
      CALL MAXCOR(BCFS,MED,MAX,NMAX)
      TYPE52,MAX,NMAX
52    FORMAT(1X,'***MAX EVECOR SIDELOBE=',I4,' ***',10X,
     1 '***NO OF OCCURENCES=',I4,'  ***')
C--------------------------------------------------------------------------
C
```

```
                               CMPTE MAX ODD CORR                        -----
C-----
C     -------------------------------------------------------------------
      MED=M
      CALL MAXCOR(OCFG,MED,MAX,NMAX)
      TYPE53,MAX,NMAX
53    FORMAT(1X,'***MAX ODDCOR SIDELOBE=',I4,' ***',10X,
     1 '***NO OF OCCURENCES=',I4,'  ***')
      GOTO3000
      STOP
      END
C<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
C-----                      SUBROUTINES                                -----
C<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
C-----      (THESE ARE EXPLAINED IN THE AO/LBE PROGRAM)                 -----
C     <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
      SUBROUTINE MAXCOR(A,ML,MAX,NMAX)
C     >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
      INTEGER A(256)
      COMMON LCMU
      NMAX=0;MAX=0
      DO 100 I=1,ML
      IF(ABS(A(I)).LT.ABS(MAX))GOTO100
      IF(ABS(A(I)).EQ.ABS(MAX))GOTO1000
      MAX=A(I);NMAX=1
      GOTO100
1000  NMAX=NMAX+1
100   CONTINUE
      RETURN
      END
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
C-----         CYSHIF PHASE-SHIFTS FC INTO FCS BY ISH                  -----
C     CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
      SUBROUTINE CYSHIF(FC,M,ISH,FCS)
      INTEGER FC(256),FCS(256)
      ISH=M-ISH
      DO 100 I1=1,M
      INC=I1+ISH
      IF(INC.GT.M)INC=INC-M
100   FCS(I1)=FC(INC)
      RETURN
      END
C######################################################################
                      SUBROUTINE CALNRO(F,J,N)
C     ##################################################################
      INTEGER F(256),BI(8),J(12)
      M=2**N
      DO 300 I=1,N
300   BI(I)=0
      DO 100 I=1,M
100   F(I)=0
      DO 200 I=1,M
      IDUM=I-1
      CALL [illegible](IDUM,BI,N)
            DO 400 K=1,N
      IF(J(K).GT.0)GOTO400
      JDUM=ABS(J(K))
      BI(JDUM)=1-BI(JDUM)
400   CONTINUE
      DO 210 K=1,N,2
      IDUM1=ABS(J(K))
      JDUM2=ABS(J(K+1))
      F(I)=(F(I)-BI(JDUM1)*BI(JDUM2))**2
200   CONTINUE
      RETURN
      END
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
                        SUBROUTINE BCONV(C,BC,N)
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
      INTEGER C,BC(8),DUMC
      DO 10 I=1,N
      DUMC=C/2
      BC(I)=C-2*DUMC
10    C=DUMC
      RETURN
      END
C*********************************************************
```

APPENDIX-C

```
C*****************************************************************
C-----  TO COMPUTE DYADIC CORRELATION BETWEEN NVAR-VARIABLE  -----
C-------  NUM-POINT p-NROFs F & G IN THEIR (1,-1)-FORMS   -------
C         -------------------------------------------------
C
C-------                   LEGEND                          ------
C-----------------------------------------------------------------
C-----  F & G ARE READ IN THEIR INDEX REPRSNTTN AS FI & GI  -----
C-----  IFWHT & IGWHT : u-WHT OF FC & GC,THE CNVRTD F & G   -----
C-----            BC : DYADIC CORRELATION                   -----
C      ******************************************************
C
      INTEGER F(256),G(256),IFWHT(256),IGWHT(256),FC(256)
      INTEGER GC(256),BC(256),FI(12),GI(12)
5000  CONTINUE
C
C-----            INPUT FI & GI AND COMPUTE F & G             -----
C      ------------------------------------------------------
      READ*,NVAR,(FI(I),I=1,NVAR)
      IF(FI(1).EQ.-1)STOP
      NUM=2**NVAR
      CALL CALNRO(F,FI,NVAR)
      READ*,NVAR,(GI(I),I=1,NVAR)
      CALL CALNRO(G,GI,NVAR)
      TYPE10,(FI(I),I=1,NVAR)
10    FORMAT(1X,'FUNCTION F',13I3)
      TYPE20,(GI(I),I=1,NVAR)
20    FORMAT(1X,'FUNCTION G',13I3)
C-----------------------------------------------------------------
C
C-----            CONVERT F & G INTO FC & GC                  -----
C      ------------------------------------------------------
      DO 300 I=1,NUM
      FC(I)=1-2*F(I)
300   GC(I)=1-2*G(I)
C-----------------------------------------------------------------
C
C-----      COMPUTE u-WHTs OF FC AND GC WITH FAST ALGRTHM      ----
C      ------------------------------------------------------
      CALL CALWHT(FC,NVAR,NUM,IFWHT)
      CALL CALWHT(GC,NVAR,NUM,IGWHT)
C-----------------------------------------------------------------
C
C-----       COMPUTE u-WHT OF BC AND TAKE INVERSE              -----
C      ------------------------------------------------------
      DO 400 I=1,NUM
400   BC(I)=IFWHT(I)*IGWHT(I)
      CALL CALWHT(BC,NVAR,NUM,BC)
      DO 500 I=1,NUM
500   BC(I)=BC(I)/NUM
      TYPE50,(BC(I),I=1,NUM)
50    FORMAT(1X,'DYAD CORR',256I5)
```

```
      STOP
      END
C
C0000000000000000000000000000000000000000000000000000000000000000000000
C----------                    SUBROUTINES                   ------------
C0000000000000000000000000000000000000000000000000000000000000000000000
C
C------   CALWHT : CMPTS u-WHT OF F USING FAST ALGORITHM       -----
C     ------------------------------------------------------------------
CGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
      SUBROUTINE CALWHT(F,NVAR,NPT,IWHT)
CGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
      INTEGER F(256),IWHT(256),PWHT(256)
      DO 100 I=1,NPT
100   PWHT(I)=F(I)
      NMID=NPT/2
      NINC=NMID+1
      DO 1000 K=1,NVAR
      DO 200 I=1,NMID
200   IWHT(I)=PWHT(2*I-1)+PWHT(2*I)
      DO 300 I=NINC,NPT
      J=2*I-NPT-1
300   IWHT(I)=PWHT(J)-PWHT(J+1)
      DO 400 I=1,NPT
400   PWHT(I)=IWHT(I)
1000  CONTINUE
      RETURN
      END
C-----------------------------------------------------------------------
C
C-----               COMPUTES NROF F FROM INDEX REP J              ------
C
C     ------------------------------------------------------------------
CDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
      SUBROUTINE CALNRO(F,J,N)
CDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
      INTEGER F(256),BI(8),J(12)
      M=2**N
      DO 300 I=1,N
300   BI(I)=0
      DO 100 I=1,M
100   F(I)=0
      DO 200 I=1,M
      IDUM=I-1
      CALL BCONV(IDUM,BI,N)
             DO 400 K=1,N
      IF(J(K).GT.0)GOTO400
      JDUM=ABS(J(K))
      BI(JDUM)=1-BI(JDUM)
400   CONTINUE
      DO 200 K=1,N,2
      JDUM1=ABS(J(K))
      JDUM2=ABS(J(K+1))
      F(I)=(F(I)-BI(JDUM1)*BI(JDUM2))**2
200   CONTINUE
      RETURN
      END
C-----------------------------------------------------------------------
```

```
C
C-----                 CONVERTS C INTO N-BIT BC                        -----
C     ---------------------------------------------------
C@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
      SUBROUTINE BCONV(C,BC,N)
C@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
      INTEGER C,BC(8),DUMC
      DO 10 I=1,N
      DUMC=C/2
      BC(I)=C-2*DUMC
10    C=DUMC
      RETURN
      END
C*************************************************************
```

APPENDIX-D
==========

```
C*****************************************************************
C------  TO FIND THE MINIMAL LFSR CKT FOR p-NROFs  -------
C     --------------------------------------------------
C
C------                 LEGEND                           ------
C----      F : p-NROF                                    ----
C----      C : THE COMPUTED CONNECTION POLYNOMIAL        ----
C     ********************************************************
      INTEGER F(256),C(256),B(256),BDUM(256),X,BD,D
      INTEGER FI(12),NPD(100),NPOD(100),T(256)
999   CONTINUE
      READ*,NUM,(F(I),I=1,NUM)
      IF(F(1).EQ.-1)STOP
C
C-----              SETTING INITIAL VALUES                 ------
C     ----------------------------------------------------------
      C(1)=1;B(1)=1;BDUM(1)=0
      DO 10 I=2,NUM
      B(I)=0;BDUM(I)=0
10    C(I)=0
      X=1;L=0;BD=1;N=0
C------------------------------------------------------------------
200   IF(N.EQ.NUM)GOTO600
      D=F(N+1)
      IF(L.EQ.0)GOTO100
      DO 20 I=1,L
      JD=N+1-I
20    D=D+C(I+1)*F(JD)
      D=D-D/2*2
100   IF(D.EQ.0)GOTO500
      LD=2*L
      IF(LD.GT.N)GOTO300
      DO 30 I=1,NUM
30    T(I)=C(I)
300   CONTINUE
      DO 41 I=1,NUM
41    BDUM(I)=0
      DO 40 I=1,NUM
      IF(B(I).EQ.0)GOTO40
      BDUM(I+X)=B(I)
40    CONTINUE
      DD=D/BD
      DO 50 I=1,NUM
      C(I)=C(I)+DD*BDUM(I)
50    C(I)=C(I)-C(I)/2*2
      IF(LD.GT.N)GOTO333
      L=N+1-L
      LJ=L+1
      DO 60 I=1,NUM
60    B(I)=T(I)
      BD=D;X=1
      GOTO400
333   LI=L+1
500   X=X+1
400   N=N+1
      GOTO200
600   DO 42 I=1,NUM
      C(I)=ABS(C(I))
      IF(C(I).LE.1)GOTO42
      C(I)=C(I)-C(I)/2*2
42    CONTINUE
C-----------------------------------------------------------)
C
C-----   CMPTING OCTAL REP OF CONN POL                  -------
C     ---------------------------------------------------
      DO 114 I=1,100
114   NPO(I)=0
      N1=(L+1)/3;N2=(L+1)-(L+1)/3*3
      DO 111 I1=1,N1
      I11=3*(I1-1)+1;I12=I11+2;NP=0
      DO 112 I2=I11,I12
      NPO(I1)=NPO(I1)+C(I2)*2**NP;NP=NP+1
112   CONTINUE
111   CONTINUE
      N3=N1+1;I13=3*(N3-1)+1;I14=L+1;NP=0
      DO 113 I3=I13,I14
      NPO(N3)=NPO(N3)+C(I3)*2**NP;NP=NP+1
113   CONTINUE
      DO 115 I=1,N3
      IS=I-1
115   NPOO(I)=NPO(N3-IS)
      TYPE1001,(F(I),I=1,NUM)
1001  FORMAT(1X,'SEQUENCE',64I2)
      TYPE2001,L,(NPOO(I),I=1,N3)
2001  FORMAT(1X,'LFSR STAGES ',I3,'
     1 'OCTAL REP OF CONN POL',100I1)
      GOTO999
555   CONTINUE
      STOP
      END
C*************************************************************
```